Zkušenosti s nasazením HW tokenů v METACentru

Michal Procházka

Daniel Kouřil

Obsah

- Úvod
- METACentrum
- Autentizace v gridech - PKI
- Autentizace v METACentru - Kerberos
- Implementace PKI do Kerbera
- HW tokeny
- Aplikace + PKI + HW token
- Distribuce tokenů

Úvod

- Sjednocení autentizačních mechanismů
  - Zjednodušit, ale nesnížit bezpečnostní úroveň
- Transparentní použití různých authentizačních mech.
- Umožnit přístup uživatelům *METACentra* do nadnárodních gridových projektů

METACentrum

- Aktivita sdružení CESNET
- Infrastruktura pro realizaci náročných výpočtů, tzv. *grid*
- 450 CPU, 25 TB distribuované diskové kapacity a 400 TB záložní páskové kapacity
- Uživatelé z různých vědních oborů
- Spoluúčast na národních a mezinárodních gridových projektech

Autentizace v gridech

- Heterogenní dynamické prostředí
- Použití PKI – *Public Key Infrastructure*
- Dvojice privátní a veřejný klíč
- Osobní certifikát
- Certifikační autority - *EUGridPMA*

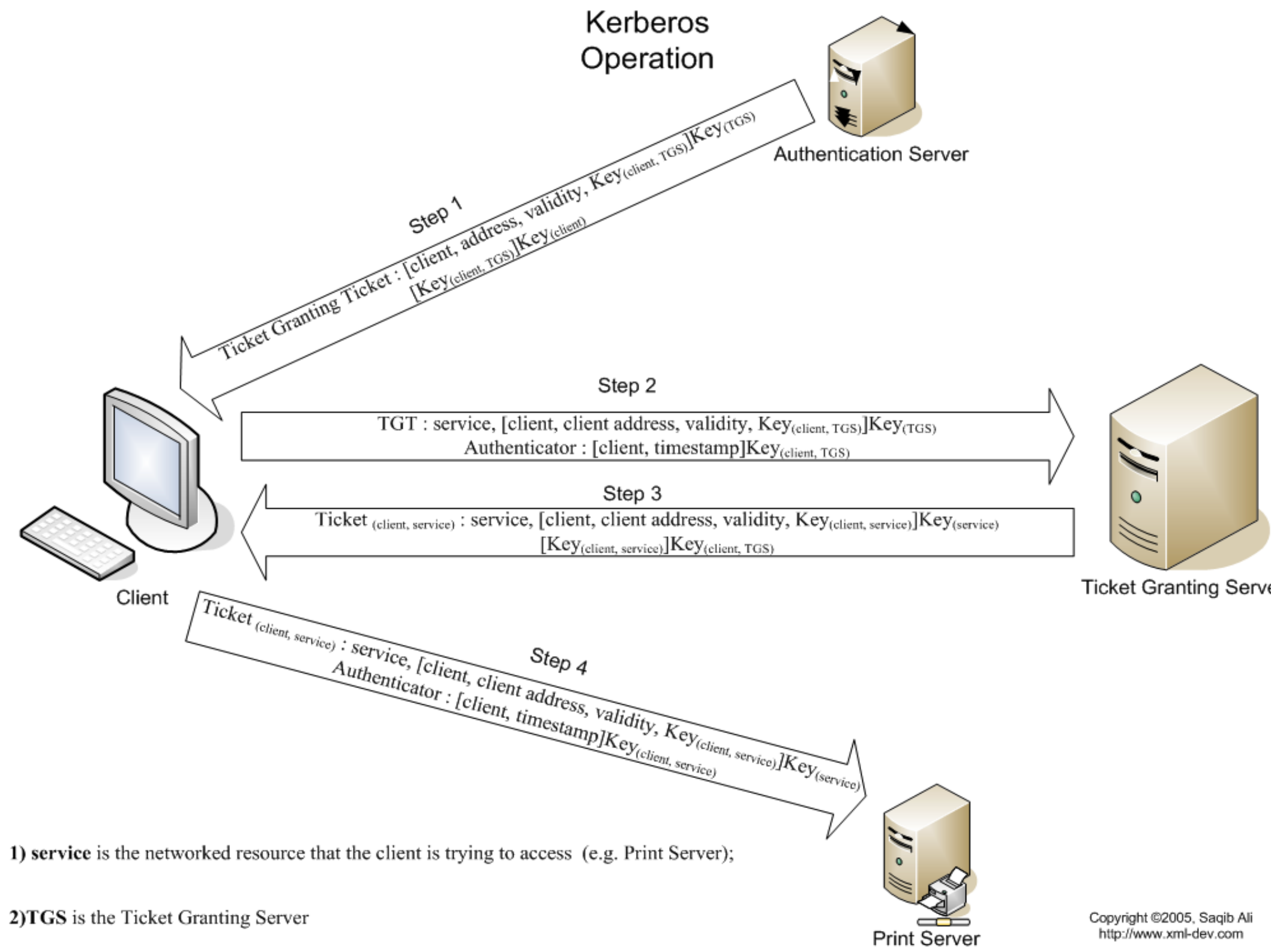
Autentizace v METACentru

- Systém Kerberos
- Bezpečná autentizace přes nezabezpečené sítě
- Využívá silné kryptografické algoritmy
- Založen na symetrické kryptografii
- Vedlejší efekt autentizace je ustavení šifrovacích klíčů
- Databáze uživatelů a služeb

Kerberos

- Kerberos lístek (*ticket*)
- Ticket Granting Ticket
- Realm a cross-realm
- Kerberos je standardizován – IETF
- Open-source implementace MIT a Heimdal
- Základní autentizační mechanismus v doménách Windows
- “pokerberizovaná” Mozilla a OpenSSH

Kerberos Operation



1) service is the networked resource that the client is trying to access (e.g. Print Server);

2)TGS is the Ticket Granting Server

Problémy PKI a Kerberos

- PKI
  - privátní klíč plně v rukou uživatele
  - nízká ochrana klíče (hesla, souborový systém, ...)
- Kerberos
  - databáze uživatelů a služeb => špatná škálovatelnost
  - pouze v METACentru

PKI a Kerberos (1)

- Požadavek minimální změny stávající infrastruktury
- Změna pouze autentizace vůči KDC serveru
- Nahrazení hesla osobním certifikátem
- Implementace PK-INIT – IETF
- kinit + OpenSSL (PKCS#11 engine)

PKI a Kerberos (2)

- Instalační balíčky – základní nástroje pro přístup k METACentru
  - program pro získávání lístků
  - ssh klienti
- Linux – SuSE, Debian, Fedora
  - OpenSSH
- Windows 2000/XP
  - Putty a WinSCP

HW tokeny

- Paměť + procesor
- Dvoufaktorová autentizace
- Bezpečné uložiště pro privátní klíč
- Čipová karta vs. USB token

Výběr HW tokenu pro METACentrum

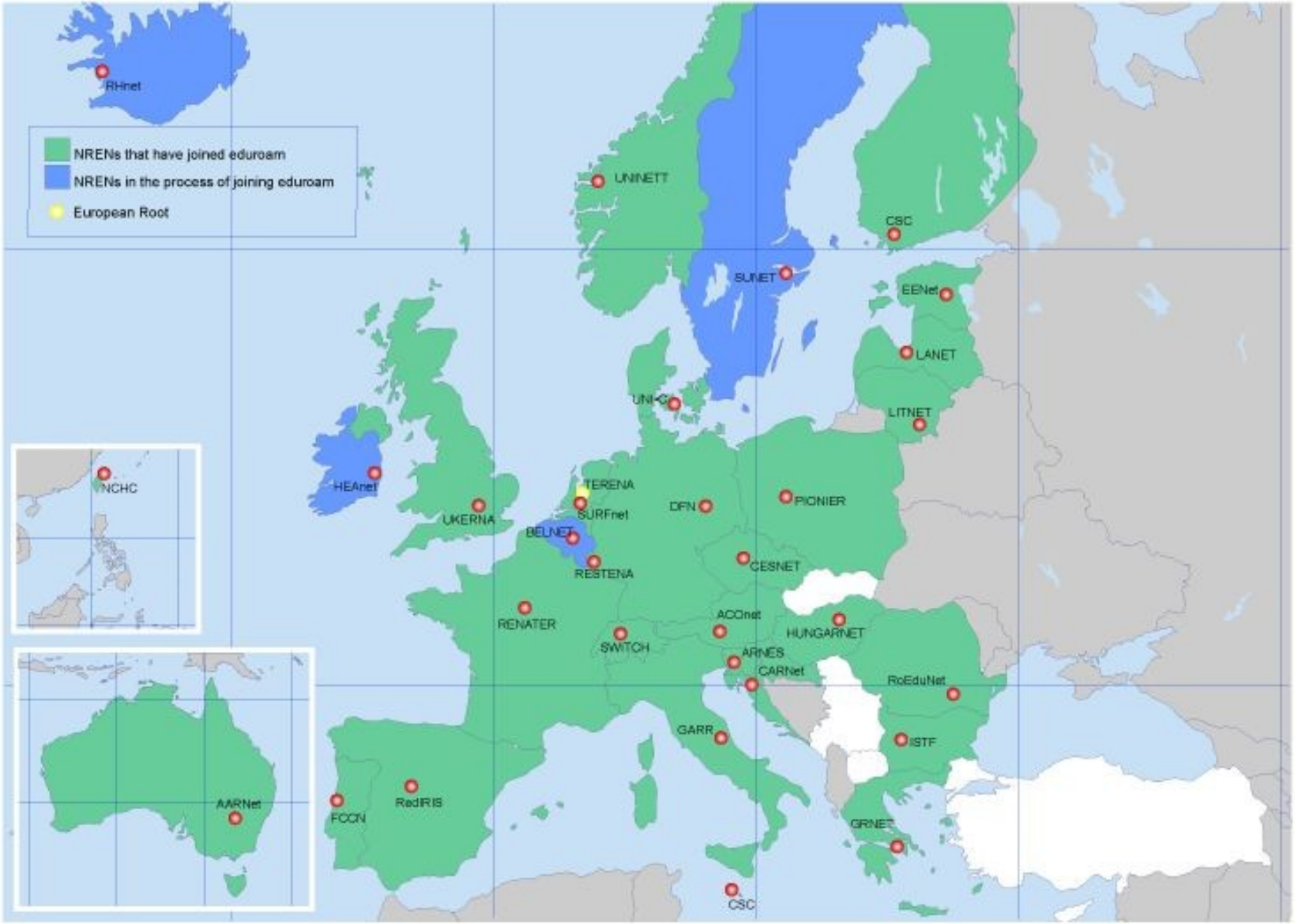
- Kritéria
  - generování klíče na tokenu, nemožnost exportu klíče
  - podpora standardů PKCS#11, PKCS#15 a MS CAPI
- Testy
  - podpora pod OS Linux/Windows
  - podpora v open-source projektu OpenSC/OpenCT
  - www prohlížeč/mailový klient

Podpora tokenů v aplikacích

- Podpora mobilních uživatelů
- VPN řešení založeno na OpenVPN
  - autentizace pomocí certifikátu na tokenu
  - dva režimy: HTTP, UDP
- Autorizace proti subjektu certifikátu

Eduroam

- Globální WiFi roaming
- 802.1x + RADIUS
- Hierarchická struktura radius serverů
- Autentizace u domovského radiusu


NRENs that have joined eduroam
NRENs in the process of joining eduroam
European Root
RHnet
UNINETT
CSC
SUNET
EENet
LANET
UNI-C
LITNET
HEAnet
NCHC
TERENA
SURFnet
DFN
PIONIER
UKERNA
BELNET
RESTENA
CESNET
RENATER
ACOnet
HUNGARNET
SWITCH
ARNES
CARNet
RoEduNet
GARR
ISTF
AARNet
RedIRIS
FCCN
GRNET
CSC

Radius a tokeny

- 802.1x – EAP
- Protokoly TTLS, PEAP, TLS
- Open-source implementace radius – Freeradius
- TLS a autorizace

Distribuce tokenů

- Certifikáty vydané CA CESNET
- Pořádaná školení
- Uživatel nerad mění návyky
- Motivace uživatelů
- Nové služby dostupné pouze za pomoci certifikátu

Budoucí práce

- Rozšíření PKI o autentizaci pomocí OTP
- Nekončící běh za výkonem...

Děkuji za pozornost