Elektronická identita – skúsenosti s certifikátmi z projektu NetC@RDS

itapa

18.11.2008

Čo je digitálny certifikát ?

- Elektronický dokument, ktorý potvrdzuje súvislosť verejného kľúča s entitou prostredníctvom digitálneho podpisu

Bezpečnostný problém

- Nedôveryhodné/neznáme prostredie
- Vzniká problém: Ako môžeme vedieť, s kým si vymieňame informácie druhej strane komunikačného kanála ?

Použitie certifikátov v rámci IS

- Prostredníctvom certifikátov sme schopní:
  - identifikovať a overiť entitu na druhej strane (používateľa, webserver, iné zariadenie..)
  - zabezpečiť dôvernosť dát (šifrovanie)
  - identifikovať, či boli dáta modifikované
  - Zabezpečiť nepopierateľnosť pôvodu dát

Project NETC@RDS

Elektronická identita

Project NETC@RDS

- Projekt NETC@RDS predstavuje iniciatívu na vybudovanie nových zlepšených služieb v rámci poskytovania zdravotnej starostlivosti

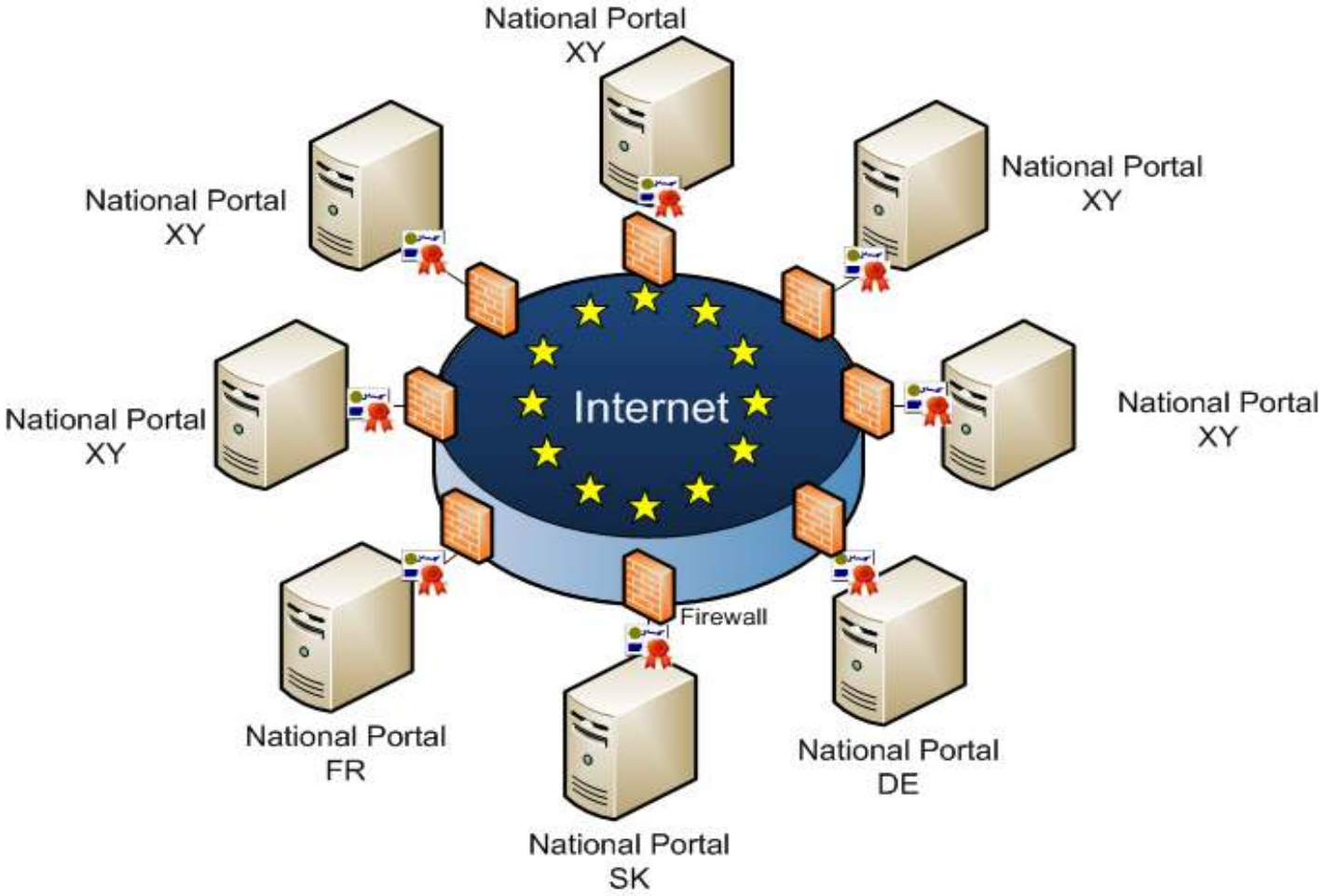
- V rámci projektu NETC@RDS sa úspešne testuje elektronická verzia EHIC (European Health Insurance Card) v 85 pilotných strediskách desiatich členských štátoch EU.

- Plánuje sa rozšírenie týchto služieb na 305 stredísk a 566 servisných miest v rámci 15-tich participujúcich krajín.

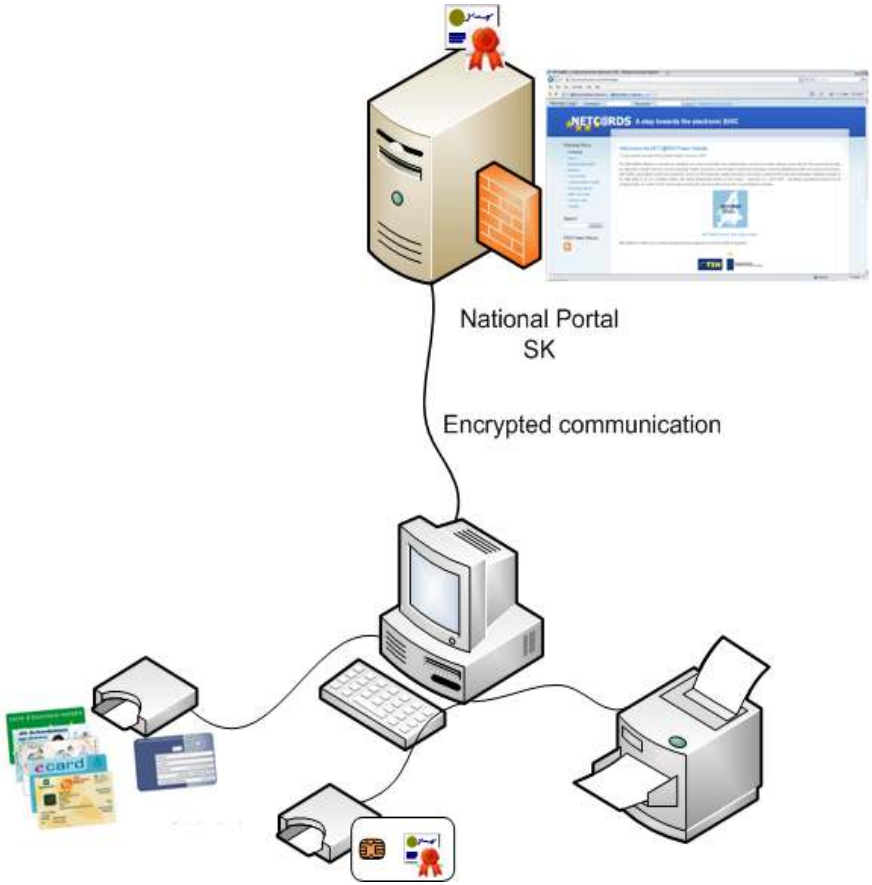
Project NETC@RDS - Elektronická identita

- Využitie digitálnych certifikátov
  - zabezpečuje identifikáciu používateľov
  - zabezpečuje identifikáciu webserverov (Národných portálov)

Project NETC@RDS – autentizácia serverov



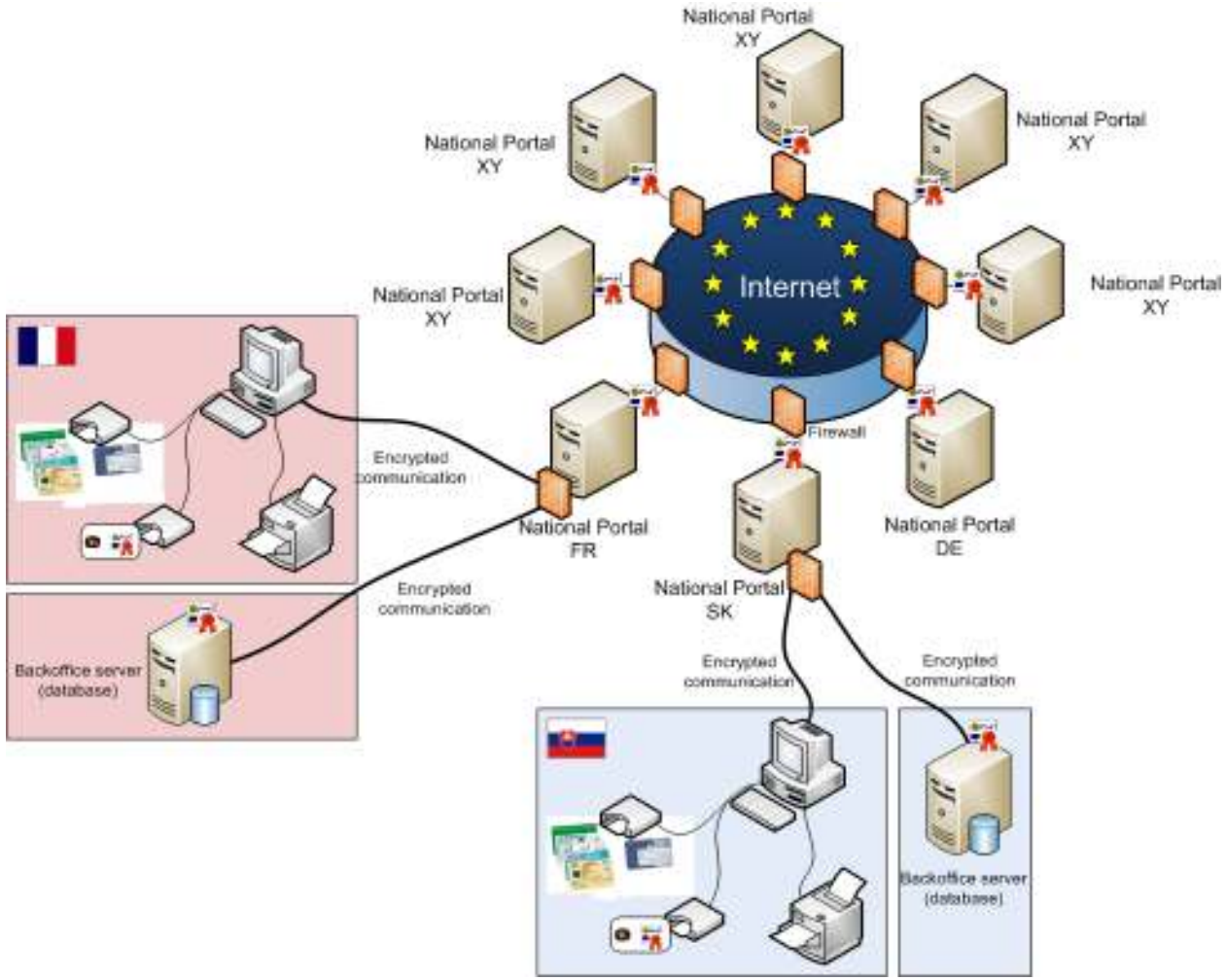
Project NETC@RDS - autentizácia používateľov



2 čipové karty:

- čipová karta používateľa (poskytovateľa zdravotnej starostlivosti)
  - autentizácia do aplikácie NETC@RDS (používateľské certifikáty, certifikát webservera – Národného Portálu),
  - Šifrovanie prenášaných dát – bezpečná komunikácia cez Internet,
- Identifikácia pacienta, úložisko dát pacienta

Project NETC@RDS – Globálna architektúra



Ochrana certifikátov a kľúčov

- Dĺžka kľúčov,
- Vhodné šifrovacie algoritmy,
- Dĺžka životnosti certifikátov,
- Ochrana prostredníctvom PIN kódu
- Používanie čipových kariet (2 faktorová autentizácia), HSM (EAL, FIPS)
- Bezpečnostný audit Certifikačnej autority (ETSI, NBÚ) v pravidelných intervaloch

Záver

Použitie certifkátov pre potreby elektronickej identity

Výhody:

- Dôveryhodnosť a používanie v rámci celej EU
- Predstavuje základ pre bezpečnostnú architektúru
- Zabezpečuje identifikáciu entity (používateľ, webserver)

Obmedzenia:

- Kľúčový manažment

di:Sig

MEMBER OF asseco GROUP

Ďakujem za pozornosť.

Otázky ???