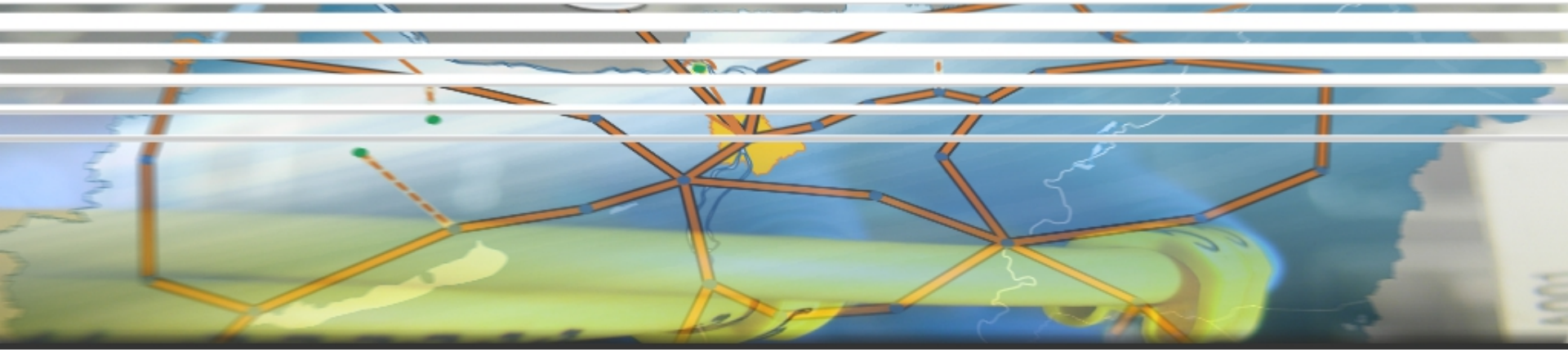
CA 2.0 light málna habbal



2014. április 25.
Pécs, Networkshop 2014

Szigeti Gábor
NIIF Intézet

Mi is az a CA szolgáltatás?

- Tanúsítvány hiteles kibocsátásért felelős eljárás.
- Műveletek:
  - Kérelem benyújtás
  - Tanúsítvány visszavonás
  - Visszavonási lista (CRL) kibocsátás
- Elérhetőség:
  - http://www.ca.niif.hu/

CA megújítás szükségessége

- 2014-ben lejár az X.509-s root tanúsítvány
- Technológia korszerűsítés

Offline vs. Online CA

- Offline:
  - kérelem beküldése
  - elbírálás
  - kérelem aláírása (+séta)
  - kiértesítés
- Online:
  - kérelem beküldése
  - elbírálás, aláírás, kiértesítés

CA megvalósítási feltételek

- EUgridPMA - www.eugridpma.org
- Hardver token használata
  - FIPS 140-2 Level 3
- Megújítási periódusok:
  - 3 év: 1024 bites kulcs
  - 5 év: 2048 bites kulcs
- Topológia:
  - Online: közvetett kapcsolat a hálózathoz
  - Offline: teljesen leválasztva a hálózatról
- 1 napos visszavonási határidő

Kitűzött célok

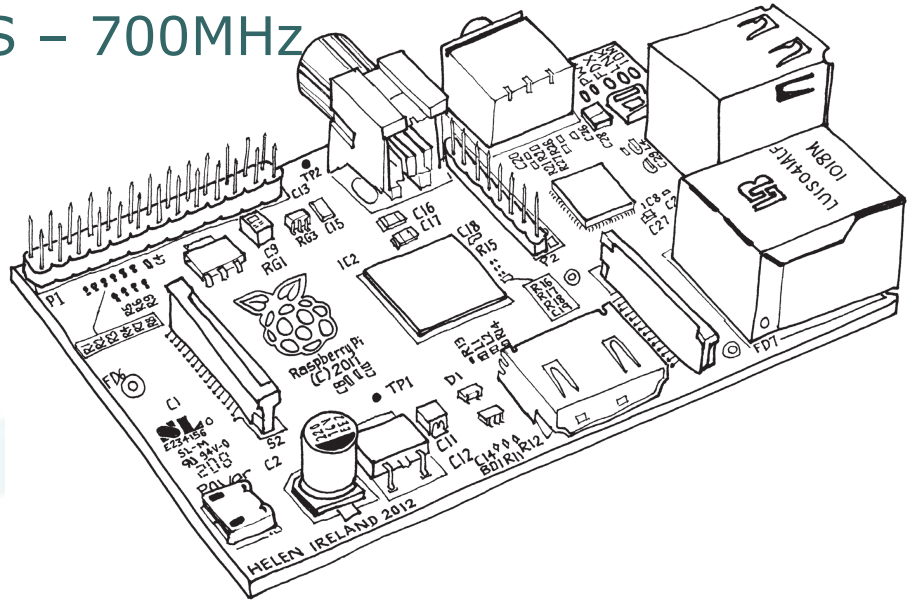
- Online megvalósítás
- 5 éves megújítási periódus
- „zöldmezős” beruházás
- költséghatékony üzemeltetés

CA megvalósítás I.

- Szoftver környezet:
  - OpenCA - http://openca.org/
  - Saját fejlesztésű szkriptek
  - Fedora 18
- Topológia:
  - PUB, RA, CA
- Hardver token:
  - Gemalto .NET IDPrime
  - Gemalto IDCore 30
  - +olvasó: IDBridge K30

CA megvalósítás II.

- Géppark:
  - Publikus rész a cloudban
  - További komponensek „alternatív” hardveren
    - RaspberryPi - http://raspberrypi.org/
      - CPU: ARM1176JZF-S – 700MHz
      - Memória: 512MB
      - Fogyasztás: 3,5W
- Hogy rakjuk a gépterembe?



Kinek ismerős?

CISCO Catalyst 2950

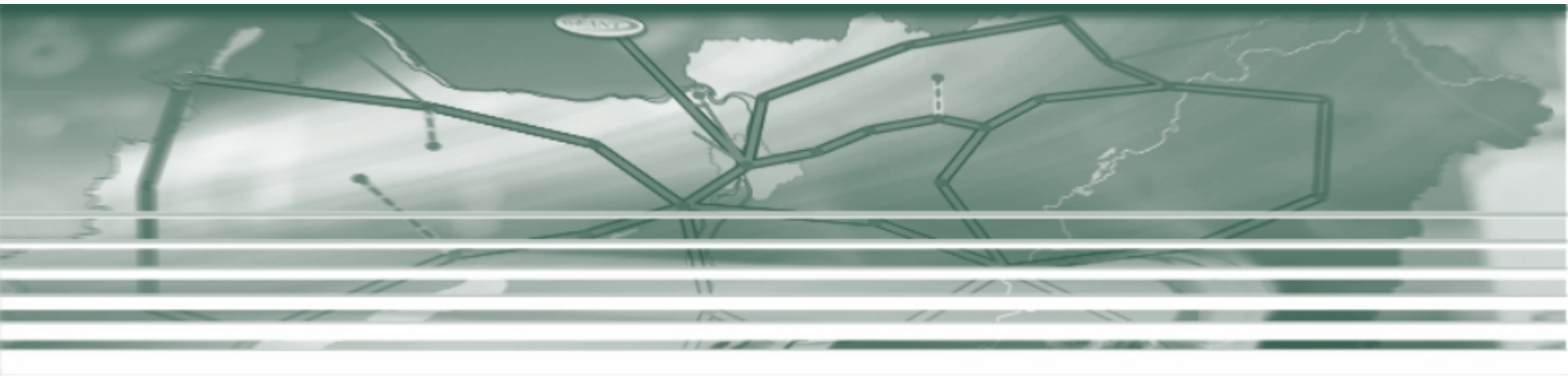
A végeredmény

- Megfelelés az Online kritériumoknak
- 2048 bites kulcs használata
- Recycling, passzív hűtés
- CA operátor a székéből se áll fel
- Üzemeltetési költségek:
  - maximum: 10Wh (87,6 kW/év)=5334Ft/év
  - minimum: 8,1Wh

Biztonsági felhívás

- OpenSSL sebezhetőségi probléma
- http://niif.hu/niif_intezet/aktualitasok/heartbleed
- Szüksége tanúsítványok visszavonása!!!

Köszönöm a figyelmet!



Szigeti Gábor
NIIF Intézet