NIIF CA szolgáltatás

HBONE tábor

2005 november

Mohácsi János <janos.mohacsi@niif.hu>

Áttekintés

- NIIF CA áttekintés
  - Fizikai környezet
  - Felépítés és működés
  - CPS/CP
- Gyakorlatban
- RMKI RA szolgáltatás

NIIF CA

- Ingyenes CA/PKI szolgáltatás a teljes akadémiai közösség számára
- Az NIIF specifikus projekt igényeinek kielégítésére: HBONE, CSIRT, GRID, stb.
- Együttműködés más CA-kal EUGridPMA és TACAR keretében

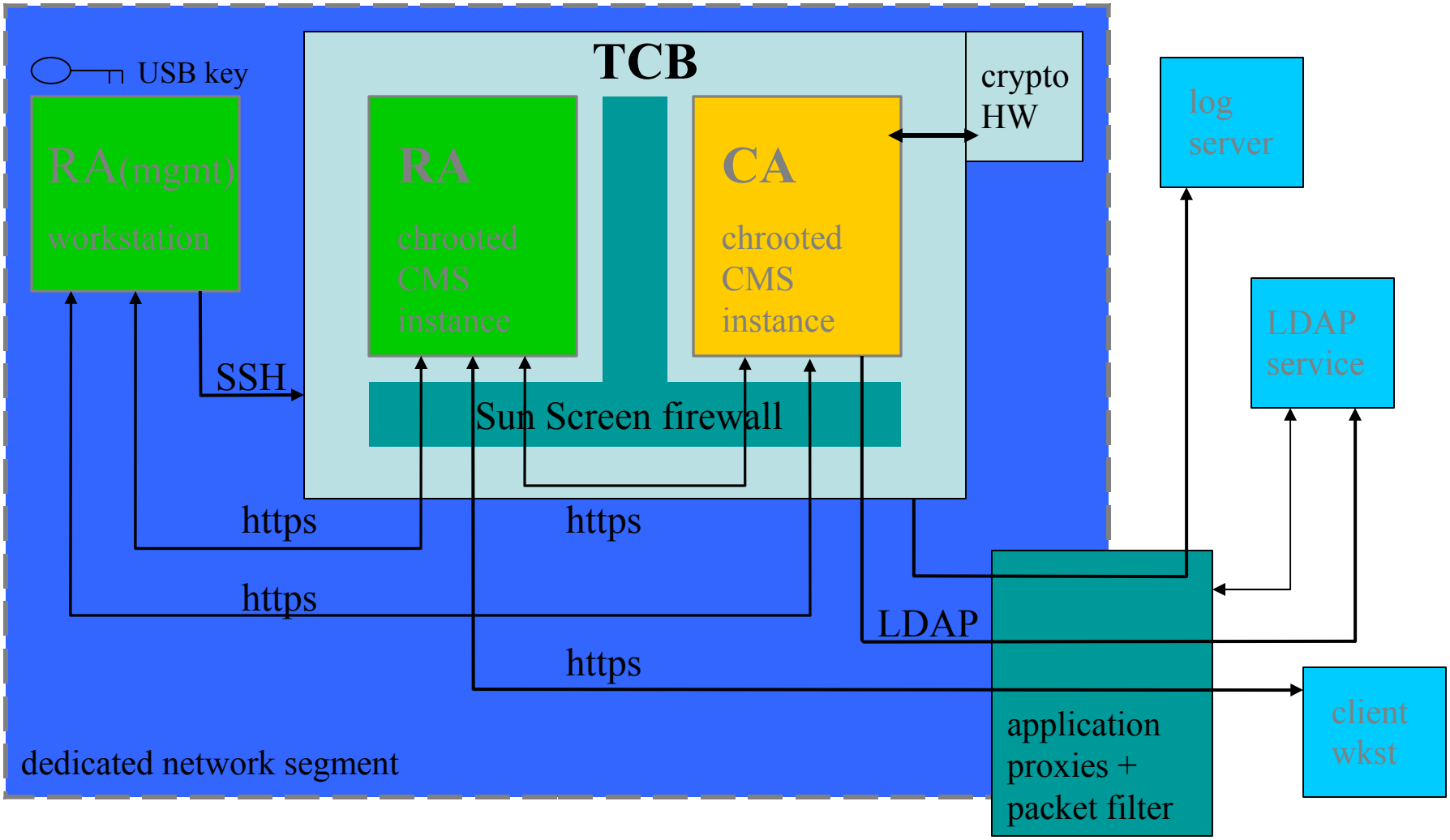
NIIF CA gép és a crypto HW

- Az NIIF CA Budapesten az NIIF központban működik
- Biztonságos környezet felügyelt környezetben

NIIF CA - Architektúra

- On-line működés – erősen ellenőrzött környezetben
- A rendszer komponensei:
  - SunFire v120, Solaris 9 OE Core, Sun ScreenLite
  - SunOne CMS
  - Chrysalis Luna crypto hardware (FIPS 140-1 Level 3)
- mgmt workstation (Linux Debian, Mozilla)
- Firewall (Linux Debian, iptables, appl. proxy)
- Certificate és CRL publikáció NIIF névtárba történik

Architektúra



CPS/CP

- 1 CPS, 4 CP (különböző alkalmazásokhoz). Egy közülük a GRID CP – leggyakrabban használt
- Nyelvek: Angolul (CPS+GRID CP), lesz magyar is
- RFC2527 és RFC3647 alapján – megfelel EUGridPMA javaslatainak és követelményeinek

CP/CPS /1

- Lehetséges több RA
- Name space: C=HU, O=NIIF CA
- Root tanúsítvány érvényessége : 10 év
- Kulcs hosszúság: 2048 bit
- A kibocsátott tanúsítvány érvényessége: 1 év + 1 hónap
- Egyéni azonosítója a felhasználóknak: email cím

CP/CPS /2

- Egyéni tanúsítvány
  - Projekthez kötődik
  - Személyes azonosító – mint egy „személyi igazolvány”
- Szerver/Eszköz tanúsítvány
  - Projekthez kötődik
  - Személy kéri

CPS/CP specialitása

- Az NIIF CA a különböző projektek igényeinek kiszolgálására lett tervezve
  - Projekt felelősök: „egy személy – az NIIF igazgatója által jóváhagyott – aki felelős a projekt adminisztrálásért”
- Projekt felelős dönti el, hogy az adott tanúsítvány igénylő jogosult-e tanúsítványt kapni az ő projektjéhez
- Csak az kaphat tanúsítványt akinek a tanúsítvány kérelmét a projekt felelős jóváhagyta – adminisztráció ketté bontása

Tanúsítvány kérelmezési eljárás /1

- A kérelmező elküldi a kérelmét papír formájában az RA- hoz. – a szükséges okmányokkal
- RA ellenőrzi, hogy a kérelmezőnek van-e jogosultsága tanúsítványt kérni – a projekt felelőssel és a dokumentációk alapján
- RA engedélyezi a kérelmező számára CAuser attribute az NIIF Névtárban – tehát előfeltétel az NIIF névtár account megléte
- RA értesíti a felhasználót a regisztrációs interfészen történő tanúsítvány kérelem módjáról

Tanúsítvány kérelmezési eljárás /2

- A kérelmező beküldi a tanúsítvány kérelmét a web-es interfészen (a publikus kulcsot is)
- A kérelmező felkeresi a regisztrációs szolgáltatót hivatali időben, hogy igazolja személy azonosságát és azt, hogy ő volt aki kérelmet beküldte
- Az RA jóváhagyja és eljuttatja a kérelmet a CA-hoz
- CA aláírja a tanúsítványt és értesíti a felhasználót e-mailben az aláírásról
- A tanúsítvány publikálásra kerül az NIIF névtárban

NIIF CA a gyakorlatban

NIIF CA felülete

URL	Tartalom
http://www.ca.niif.hu/rootkey.html	The NIIF CA root tanúsítvány
http://www.ca.niif.hu/en/policies/	CP/CPS-ek elérhetősége
http://www.ca.iif.hu/crl/niif-ca-crl.crl	Visszavonási lista
http://ocsp.ca.niif.hu:2560/	OCSP responder funkció
http://www.ca.niif.hu/niif_ca_howtoget.h	Leírás
https://register.ca.niif.hu	Regisztrációs interfész – csak authentikációval érhető el
http://www.ca.niif.hu/niif_ca_ra.html	RA információk

NEMZETI INFORMÁCIÓS INFRASTRUKTÚRA FEJLESZTÉSI IRODA

NIIF CA Pre-Authorization Request form

Certification Request **Date:** .....

To: <RA NAME> **NIIF CA RA**
<RA ADDRESS> **Victor Hugo u. 18-22., H-1132, Budapest, HUNGARY**

Section 1 – Requestor's details

Requestor's Name: .....

E-Mail Address: .....

Phone Number: .....

Common Name (CN)*: .....
* full name (given name, family name) in case of personal certificate, or FQDN in case of server/device certificate

Organisational users only:

Organisation (O): .....

Department (OU): .....

Requestor's data in the NIIF Directory:
☐ I am included in the NIIF Directory ☐ I am not included in the NIIF Directory ☐ I don't know

Type of requested certificate:
☐ – Grid ☐ – HBONE ☐ – CSIRT ☐ – General purpose

The certificate planned to be used for (check only one):
☐ - End User Certificate ☐ – Server/Device Certificate

Section 2 – Reason for request:

.....

.....

Section 3 – Attached documents:

☐ Copy of the Photo – ID
☐ Statement about the employment status at the organization (In case of general purpose certificate)
☐ Data Protection Information and Statement form (In case of requestor not included in the NIIF Directory)
☐ Statement about the domain name ownership (In case of server certificate)
☐ Statement about the domain name usability (In case of server certificate)
☐ Other .....

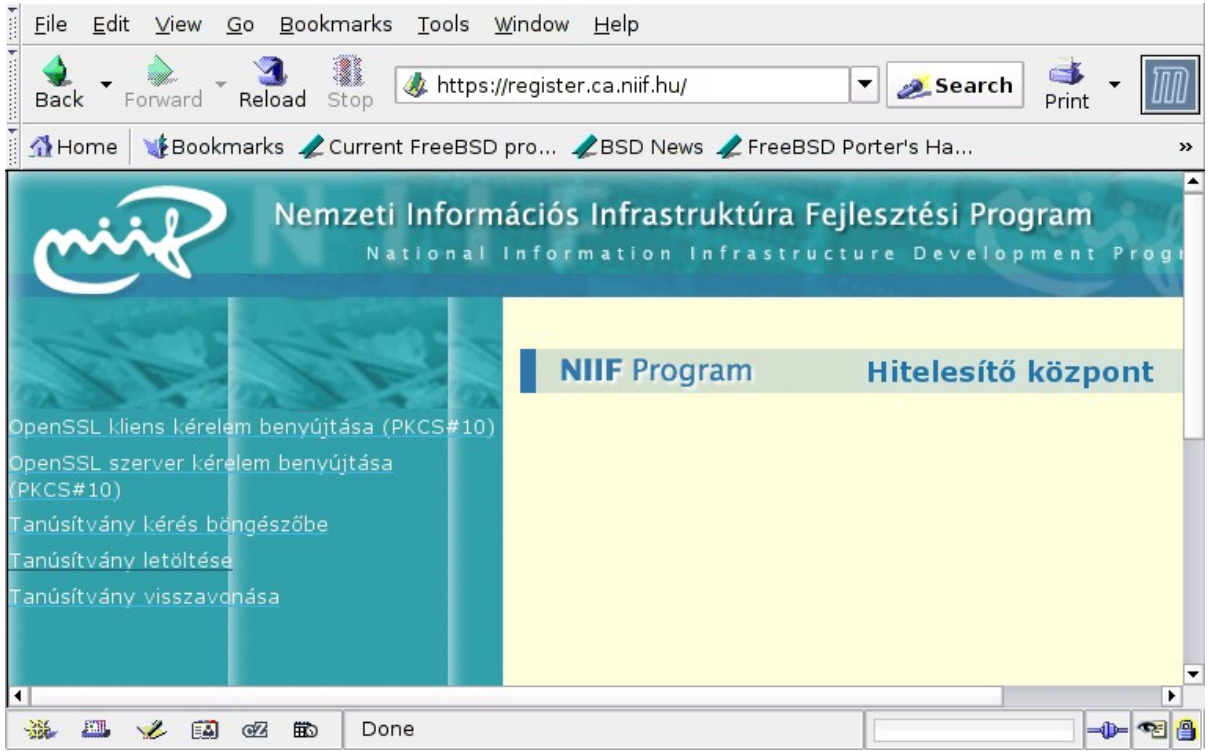
I know and accept all the rules and obligations described in the NIIF CA CPS/CP documents under which authority the requested certificate is going to be issued.

Signature: .....

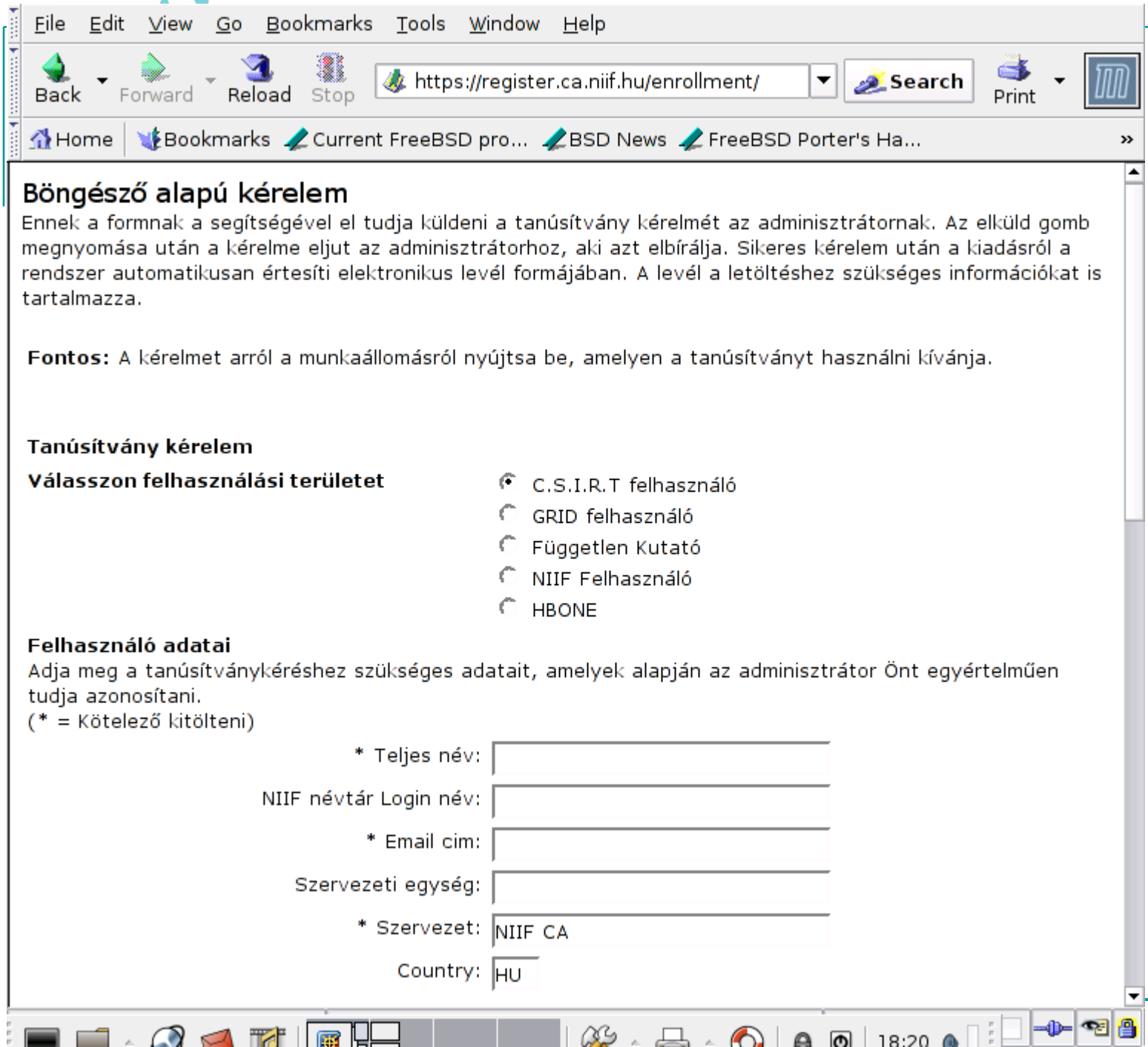
Jóváhagyás

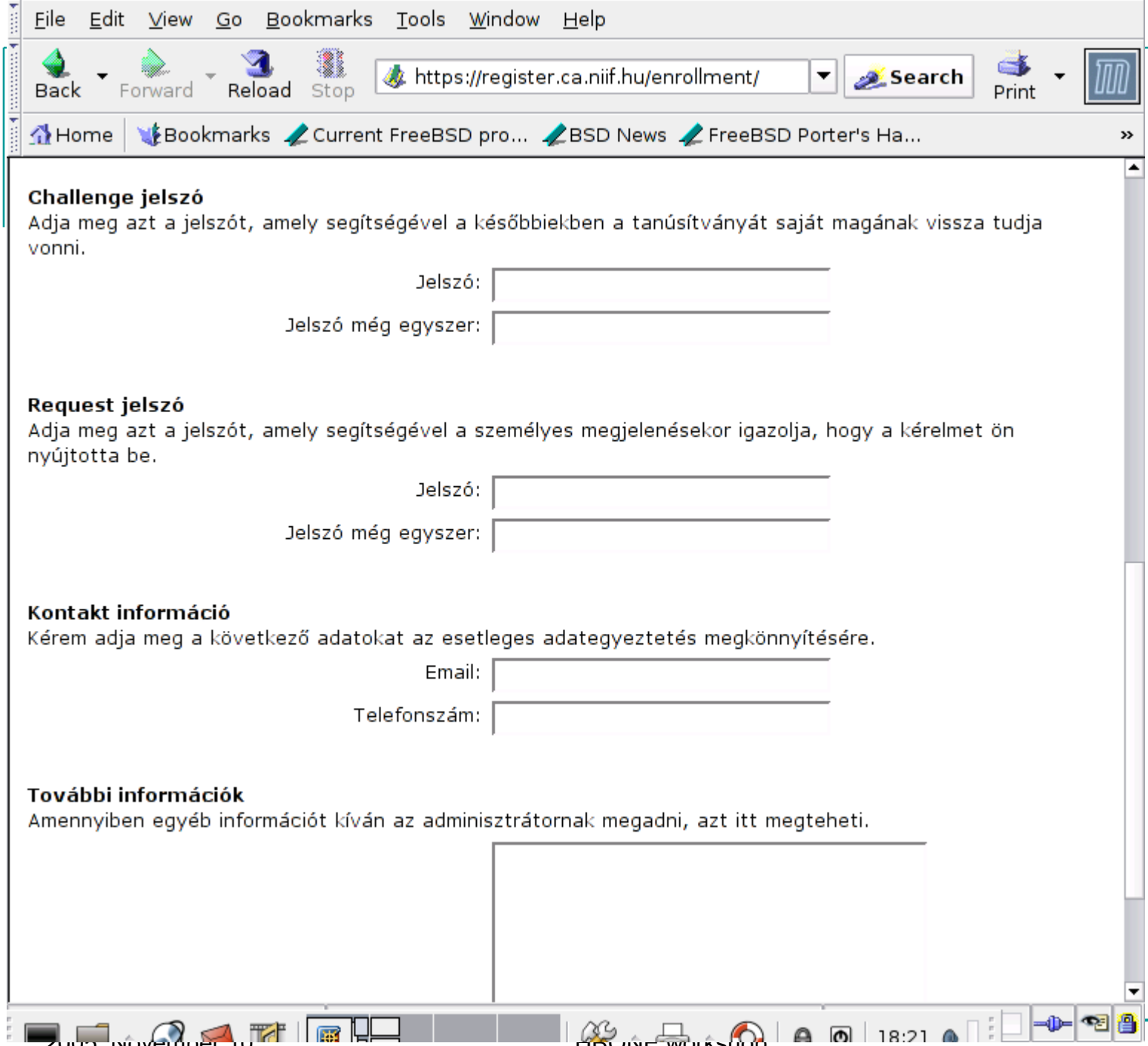
- Projekt felelős, aki engedélyt ad az adott projekthez kapcsolódó tanúsítvány kiadására
  - GRID személyes tanúsítvány – GRID projekt vezető (Stefán Péter)
  - CSIRT személyes tanúsítvány – CSIRT vezető (Mohácsi János)
  - NIIF személyes tanúsítvány – Elektronikus levelezés szolgáltatás felelős (Máray Tamás)
  - HBONE személyes tanúsítvány – HBONE üzemeltetés (Springer Ferenc)

Regisztrációs interfész



Authentikácó e-mail címmel és NIIF névtár jelszóval!


File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
https://register.ca.niif.hu/enrollment/
Search
Print
Home Bookmarks Current FreeBSD pro... BSD News FreeBSD Porter's Ha...
Böngésző alapú kérelem
Ennek a formnak a segítségével el tudja küldeni a tanúsítvány kérelmét az adminisztrátornak. Az elküld gomb megnyomása után a kérelme eljut az adminisztrátorhoz, aki azt elbírálja. Sikeres kérelem után a kiadásról a rendszer automatikusan értesíti elektronikus levél formájában. A levél a letöltéshez szükséges információkat is tartalmazza.
Fontos: A kérelmet arról a munkaállomásról nyújtsa be, amelyen a tanúsítványt használni kívánja.
Tanúsítvány kérelem
Válasszon felhasználási területet
C.S.I.R.T felhasználó
GRID felhasználó
Független Kutató
NIIF Felhasználó
HBONE
Felhasználó adatai
Adja meg a tanúsítványkéréshez szükséges adatait, amelyek alapján az adminisztrátor Önt egyértelműen tudja azonosítani.
(* = Kötelező kitölteni)
* Teljes név:
NIIF névtár Login név:
* Email cim:
Szervezeti egység:
* Szervezet:
NIIF CA
Country:
HU
18:20


File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
https://register.ca.niif.hu/enrollment/
Search
Print
Home Bookmarks Current FreeBSD pro... BSD News FreeBSD Porter's Ha...
Challenge jelszó
Adja meg azt a jelszót, amely segítségével a későbbiekben a tanúsítványát saját magának vissza tudja vonni.
Jelszó:
Jelszó még egyszer:
Request jelszó
Adja meg azt a jelszót, amely segítségével a személyes megjelenésekor igazolja, hogy a kérelmet ön nyújtotta be.
Jelszó:
Jelszó még egyszer:
Kontakt információ
Kérem adja meg a következő adatokat az esetleges adategyeztetés megkönnyítésére.
Email:
Telefonszám:
További információk
Amennyiben egyéb információt kíván az adminisztrátornak megadni, azt itt megteheti.
18:21

RMKI RA szolgáltatás

RMKI RA szolgáltatási terv

1. Igények felmérése
2. Megállapodás KFKI RMKI és NIIF között
3. KFKI RMKI CA nem ad ki több grid tanúsítványt, de tovább működik amíg van érvényes kibocsátott tanúsítványa
4. KFKI RMKI RA lesz NIIF CA-ban

Köszönöm

Várjuk a tanúsítvány kérelmeket…

És az ötleteket, hogy hol szeretnétek tanúsítványokat használni