

CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA

Implementation of open-source PKI solution

CARNet PKI

DAMIR REGVART

28.09.2004

Contens:

- 1. PKI in 60 sec
- 2. PKI solution in CARNet
- 3. Future development

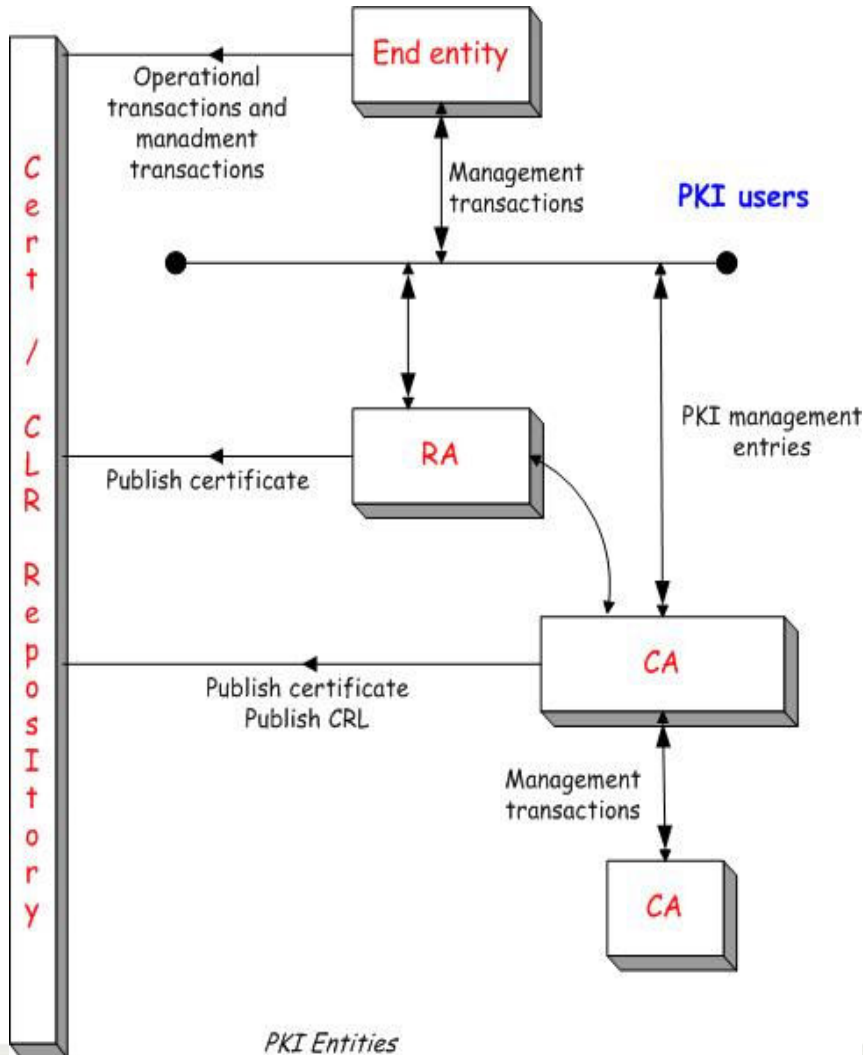
1. PKI in 60 sec

- Public key infrastructure (X.509: RFC 2459 & updated RFC 3280),
- strong hierarchical organization,
- Term used to describe:
 - policies, standards, software requirements...
 - regulation of public & private pairs of keys
- System of digital certificates, Certification Authority (CA) & Registration Authority (RA)
- off-course: use of cryptography!

Uses of PKI:

- SSL, IPsec, HTTPS – communication & transaction
- S/MIME & PGP – email security
- SET – value exchange
- Benefits:
 - Reduces transactional processing expenses,
 - Reduces the complexity of security systems,
 - Notarization (contracts, emails...)
 - In software distribution (signing applications...)

Parts of PKI infrastructure:



- > Node for management (database)
- > CA (Certification Authority)
- > RA (Registration Authority)
- > Repository (LDAP)
- > Public part for users of PKI (CSR, certificate signing request)
- > SCEP (*from ver. 0.9.2-RC-6*)

2. PKI in solution in CARNet

Why implement PKI in CARNet?

- ▶ Goals:
 - ▶ Improvement in secure communications
 - ▶ Replacements of students ID cards (X-ica)
 - ▶ Unique and simplified method of student identification (for authentication and authorization...)
- ▶ Implementation of “Open Source PKI solution”:
OpenCA (why?)
 - ▶ Totally free (open-source),
 - ▶ Customization for CARNet needs,
 - ▶ but still in development phase...
 - ▶ based on X.509
- ▶ Integration with smart card for better security

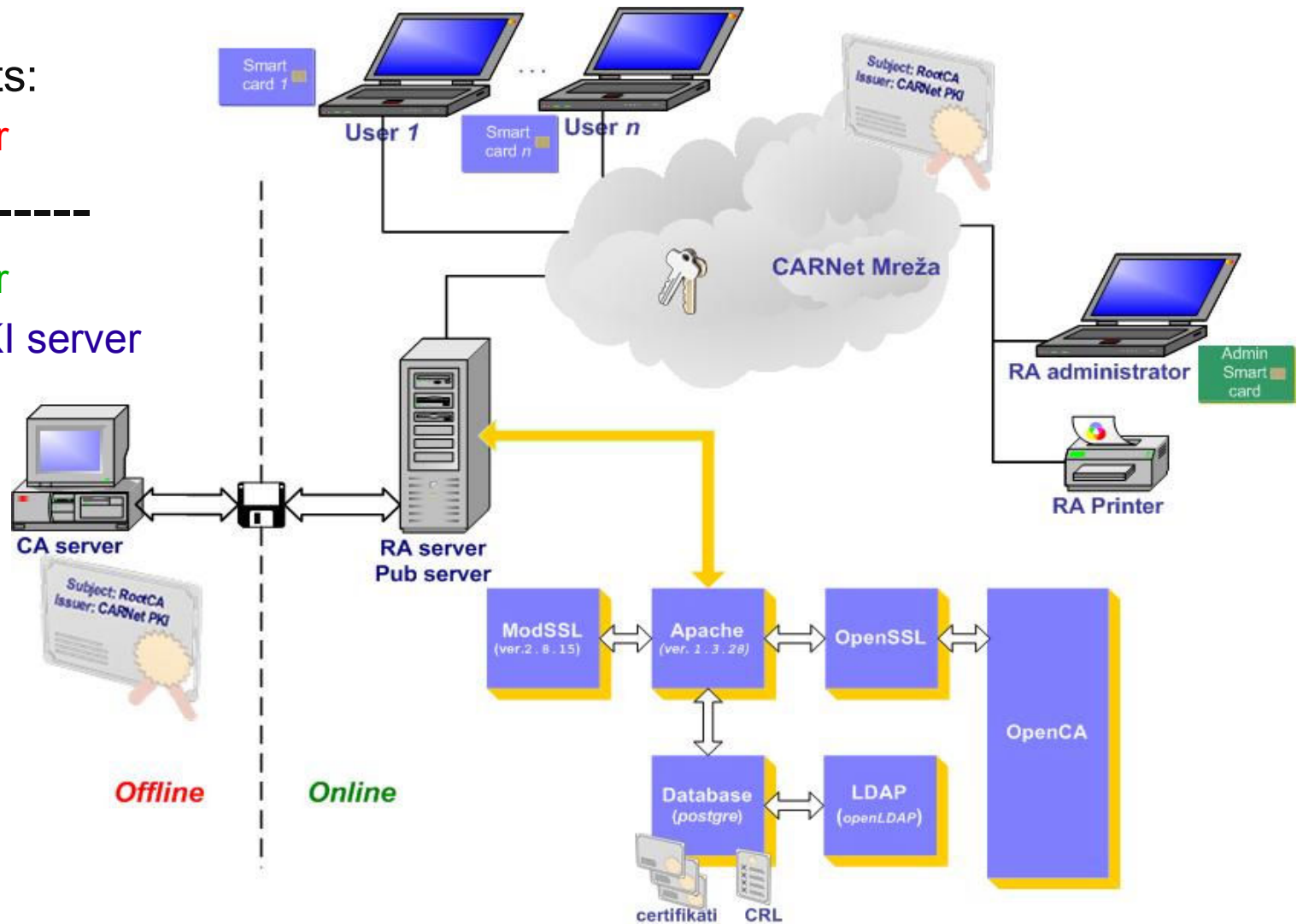
Topology of CARNet PKI

> PKI elements:

- CA server

- RA server

- Public PKI server



What user receives from CARNet PKI?

- Private key,
- Public key,
- Certificate,
- Smart card (iCAR),
- Reader for smart card,
- Tools for management of smart card.

Contents of smart card

The screenshot displays two windows from a smart card management application. The top window, titled "Program za upravljanje tokenom", shows the name of the cardholder as "Damir Regvart" and the token status as "operativan". The bottom window, titled "PKCS #11 objekti", provides detailed information about the token and its contents.

Informacija o tokenu:

Polje	Vrijednost
Oznaka tokena	Damir Regvart
Serijski broj tokena	2325003701901809
Dovršavanje nizova	ne
PIN stanje	U redu
PUK stanje	U redu
Duljina PIN-a	Maksimalno 8 znakova/minimalno 4 znakova
Javna memorija	Ukupno 4608 byteova/Slobodno 1372 byteova/Zauzeto 3236 byteova
Privatna memorija	Ukupno 512 byteova/Slobodno 512 byteova/Zauzeto 0 byteova

Sadržaj tokena

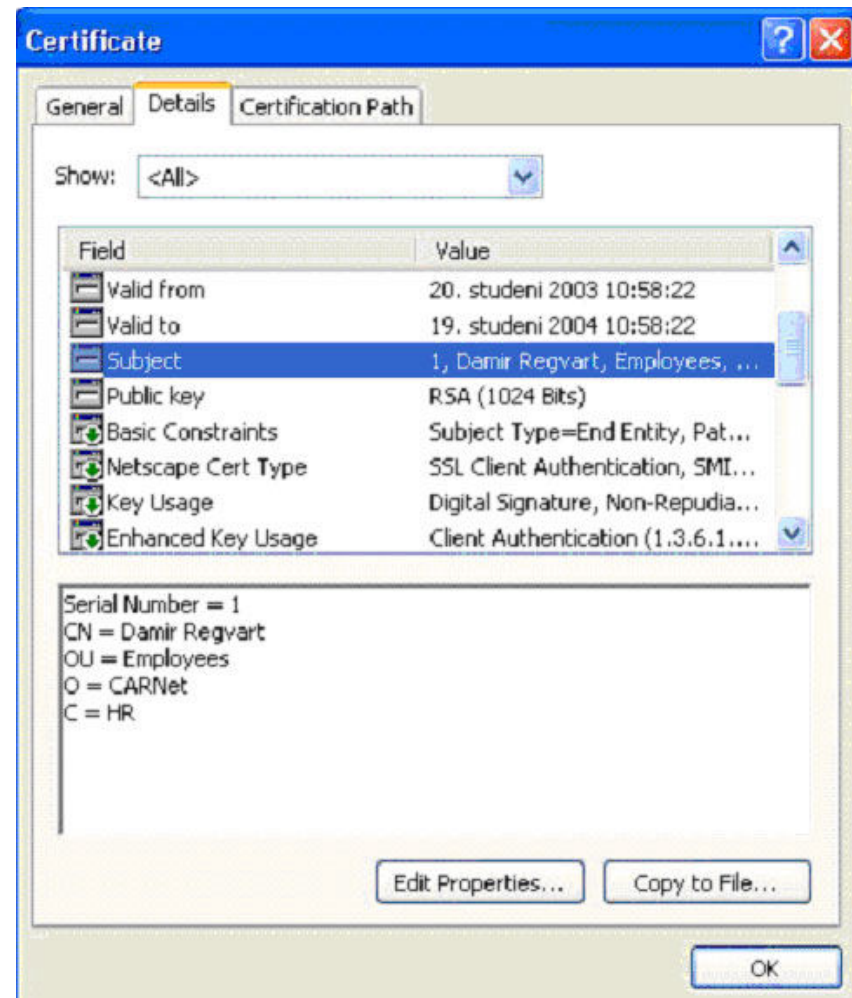
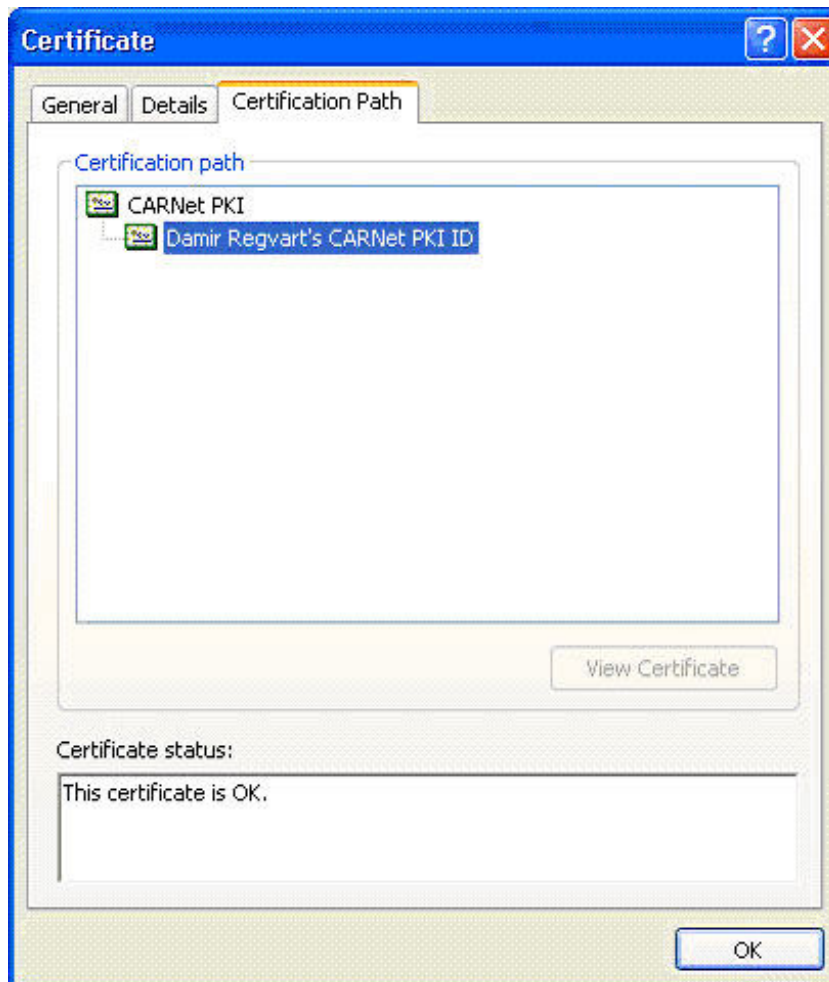
Objekti:

Vrsta	Oznaka	Privatni
Certifikat	Damir Regvart CARNet PKI ID	ne
Certifikat	CARNet PKI	ne
Certifikat	Reggie CARNet PKI ID	ne
Privatni ključ	Damir Regvart CARNet PKI ID	da
Privatni ključ	Reggie CARNet PKI ID	da

Trajanje učitavanja: **1.77 sekundi**

Izbrisi objekt Prikaži certifikat Prikaži sve objekte Zatvori

Contents of CARNet certificate:



What could user do with CARNet PKI?

- Testers of CARNet PKI are CARNet workers :-)
- PKI in CARNet is in test phase...
- What can users do:
 - Signing e-mails (S/MIME),
 - Signing documents,
 - Logon to Windows domain,
 - Logon to secure WebPages (**https**) & internal CARNet applications,
 - Logon to VPN concentrator (usin PKI to establish VPN connection),
 - Logon to computer (*Linux enabled*)

3. Future development of CARNet PKI

- ▶ Finale goal:
 - ▶ Replacement of students ID cards with smart cards,
 - ▶ Unique and simplified method of identification for authentication and authorization
 - ▶ Personal e-ID (*in 5 years*)
- ▶ Future CARNet PKI projects:
 - ▶ Digitally sign every server in CARNet network,
 - ▶ PKI pilot implementation project in selected Campus...
 - ▶ Working on AAI project for CARNet network
 - ▶ Working in OpenCA project

For more information go to:

- Carnet PKI web page: <http://pki.rdlab.carnet.hr>
- OpenCA project: <http://www.openca.org>
- M.U.S.C.L.E: <http://www.linuxnet.com/>
- Public-Key Infrastructure (X.509) (pkix) charter:
<http://www.ietf.org/html.charters/pkix-charter.html>

Q & A...