Certreq: a standalone tool for certificate requests generation and certificates retrieving in GRIDNNN

Yu.Yu. Dubenskaya[1], A.P. Kryukov[2],
L.V. Shamardin[3]

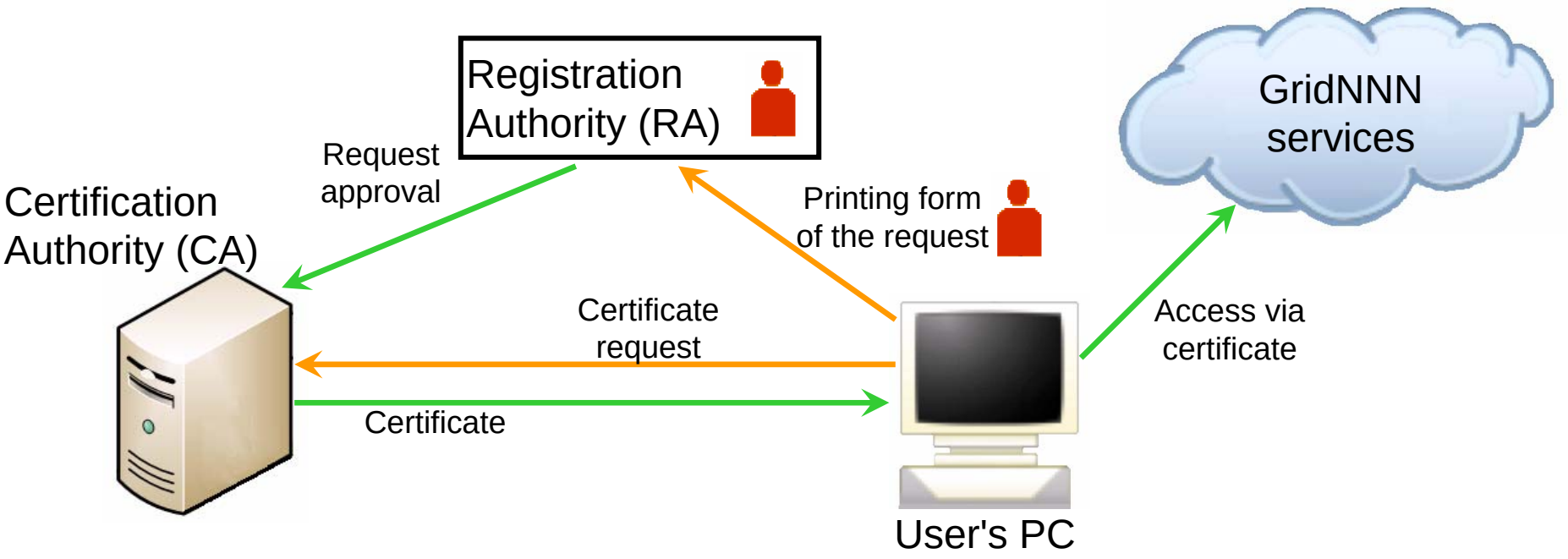
Scobeltsyn Institute of Nuclear Physics
Lomonosov Moscow State University

1) dubenskaya@theory.sinp.msu.ru, 2) kryukov@theory.sinp.msu.ru, 3)shamardin@theory.sinp.msu.ru

The work was partially supported by Ministry of Education and Science (Contract No 07.514.11.4022),
RFBR (Grant No 11-07-00434-a), Grant council of President of RF (NSh-3920.2012.2)

Authentication and authorization in GridNNN

- The security concept of GridNNN is fully based on a public key infrastructure (PKI)
- To be able to send any request to services every GridNNN user has to obtain his/her personal X.509 certificate



Certificate obtaining procedure in GridNNN

Requirements and restrictions

- A private key and a certificate request must be generated on the user's computer
- Filling of the printing form of the request with key modulus is manual and thus error-prone
- Request generation step requires use of the OpenSSL cryptographic library
- Replacement of the previously used certificate and private key with the new ones is a manual procedure
- To prepare a certificate request correctly user has to understand the certificate issuance workflow and perform all the steps in the right order

Usability: points to improve

- Certificate obtaining should be as automated as possible:
  - gathering of user data; key and request generation; preparing and filling of the printing form; request uploading to the CA should be done automatically at one step
  - download of the issued certificate, replacement of the obsolete certificate and private key with the new ones, archiving of the previous credentials (if needed) should be done automatically at one step as well
- Certificate obtaining should not require special skills in PKI and its specific implementations in Windows and/or Unix operating systems

Usability vs security

- Overall security of the network should not be reduced

Goal

Provide users with an easy-to-deal-with tool for managing their certificates and certificate requests that does not require modifications of the existing infrastructure

Solution: Certreq

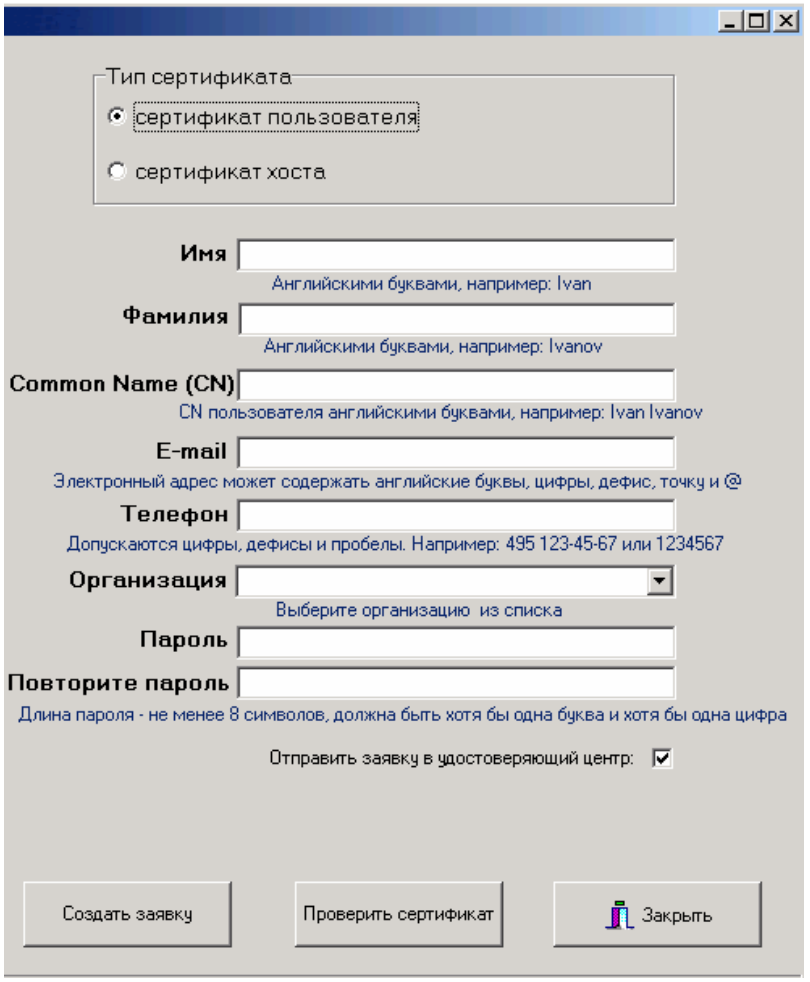
- Certreq is a standalone tool for management of keys and certificates
- No installation and/or configuration needed
- What to do to get the program working:
  - download program archive;
  - unpack it on the local computer;
  - run the program file: certreq.py (on Unix) or certreq.exe (on Windows)

Certreq features

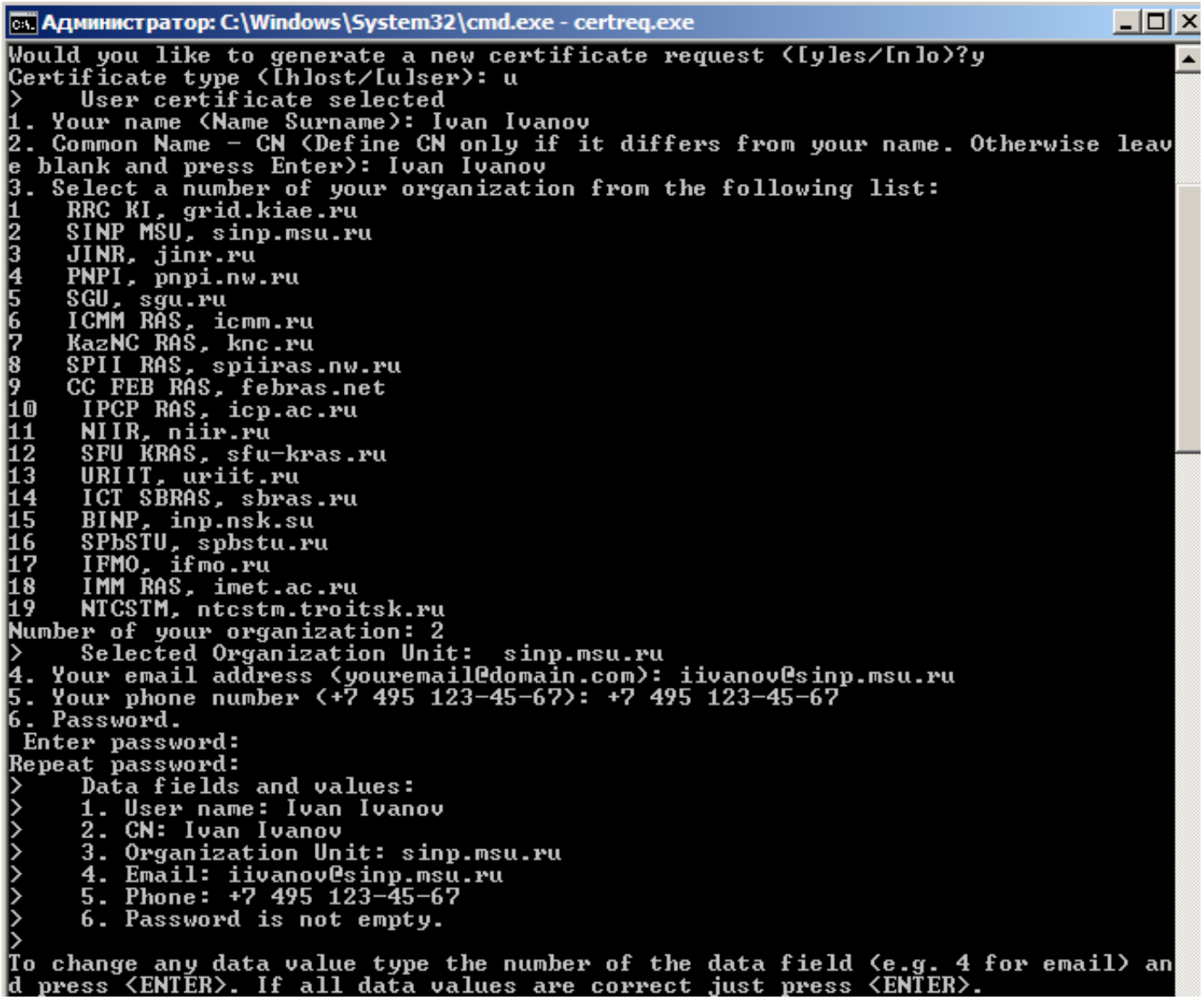
- Certificate requests management
  - create new certificate request
  - prepare the printing form of the request
  - upload certificate request to the CA
- Certificates management
  - retrieve issued certificate from the CA
  - archive previously used private key and certificate
  - save downloaded certificate to the default location under the default name
  - export of the private key and certificate in pkcs12 format
  - import of the private key and certificate from pkcs12 format

Certreq modes of operation

- Graphical interface
- Command line interface
  - interactive mode
  - non-interactive mode (all parameters are set via options)



Example of the interactive mode



Command line options

certreq.exe

--genr	// create a new certificate request
--host	// create host request
--upload	// upload request to to the CA
--cn *common_name*	// CN of a user or of a host
--username *user_name*	// User name of a user or of a host administartor
--ou *organization_unit*	// Organization unit
--email *user_email*	// E-mail of a user or of a host administartor
--phone *user_phone*	// Phone number of a user or of a host administartor
--password *user_password*	// Password
--checkcert	// Retrieve issued certificate from the CA
--rewrite	// Save downloaded certificate to the default location
--export *file_name*	// Export certificate and private key to the pkcs12 file
--import *file_name*	// Import certificate and private key from the pkcs12 file
--reqname *file_name*	// Check if certificate for the specified request has // already been issued and if so download that certificate

Example. Request a host certificate:

certreq.exe --genr --host --upload --cn *test26.ngrid.ru* --username *"Ivan Ivanov"* --ou *sinp.msu.ru* --email *iivanov@sinp.msu.ru* --phone *"+7 495 123-45-67"*

Links

- Certreq is used in GridNNN project (***www.ngrid.ru***)
- Certreq is written on python language (***www.python.org***)
- OpenSSL library is included in the program distribution (***www.openssl.org***)
- py2exe was used to prepare certreq.exe file for Windows (***www.py2exe.org***)

Alternative solution

- Certificate authority with highly functional web-interface. As an example of such a CA OpenCA project (www.openca.org) can be considered

Pros

- Web-interface has a wide functionality to create certificate requests and download issued certificates in the interactive mode
- The only program a user should install is a web browser
- Server-side checks of the user data ensure compliance with the certificate policy

Contras

- By security reasons there is no possibility to automatically put an issued certificate to the default location in the file system on user's PC
- Some servers do not provide any interface for non-interactive requests
- In GRIDNNN the solution implies modification of the existing CA implementation and thus is beyond the scope of this work

Conclusion

- Certreq facilitates management of the certificate requests and certificates:

  - after request generation the printing form is prepared and filled while the request is uploaded to the CA

  - Certreq automatically checks all the actual user requests and downloads issued certificates

  - previously used key and certificate could be archived (if needed)

  - there is no need to install any cryptographic libraries and/or other programs

- Certreq offers several modes of operation:

  - non-interactive command line

  - interactive command line

  - graphical interface

- Usability improving is achieved by automating manual operations and the PKI is not modified

Thank you!

Questions/Comments?