

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

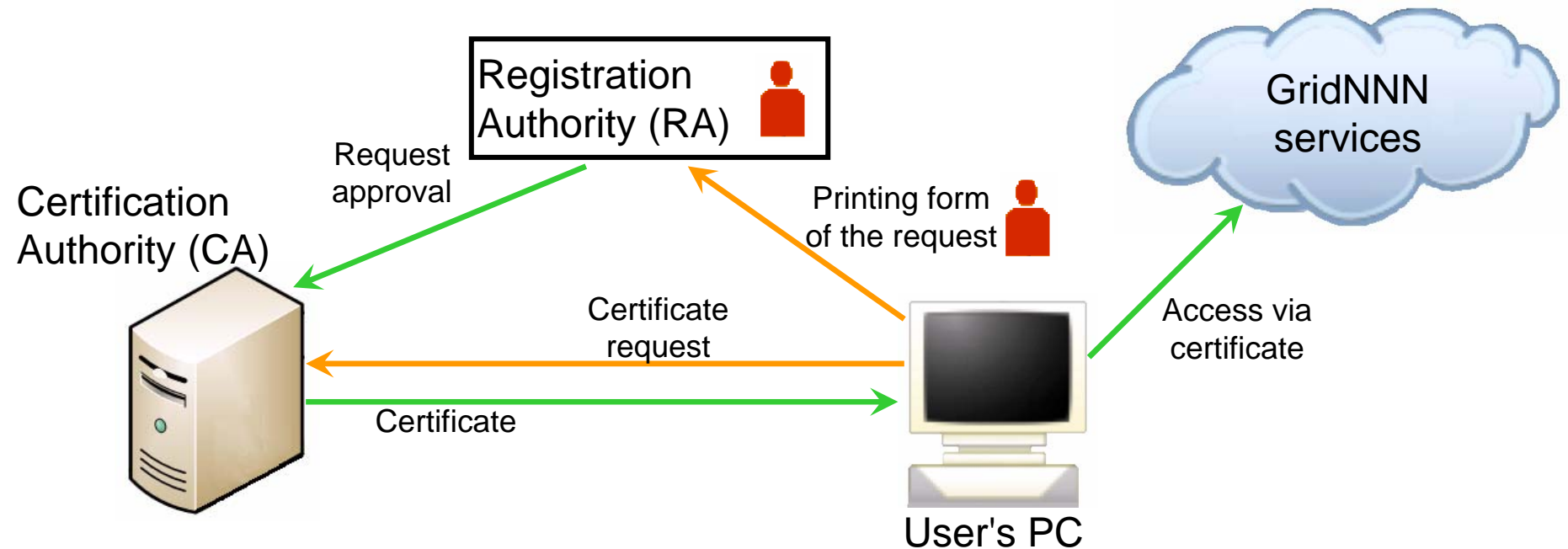
Yu.Yu. Dubenskaya<sup>1</sup>, A.P. Kryukov<sup>2</sup>,  
L.V. Shamardin<sup>3</sup>

Scobeltsyn Institute of Nuclear Physics  
Lomonosov Moscow State University

1) [dubenskaya@theory.sinp.msu.ru](mailto:dubenskaya@theory.sinp.msu.ru), 2) [kryukov@theory.sinp.msu.ru](mailto:kryukov@theory.sinp.msu.ru), 3) [shamardin@theory.sinp.msu.ru](mailto:shamardin@theory.sinp.msu.ru)

# 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)

The screenshot shows a graphical user interface for generating a certificate request. It features several input fields and a radio button selection for the certificate type. The fields include: 'Имя' (Name), 'Фамилия' (Surname), 'Common Name (CN)', 'E-mail', 'Телефон' (Phone), 'Организация' (Organization), 'Пароль' (Password), and 'Повторите пароль' (Repeat password). A checkbox at the bottom indicates whether to send the request to a trusted center. At the bottom of the window are three buttons: 'Создать заявку' (Create request), 'Проверить сертификат' (Check certificate), and 'Закреть' (Close).

Тип сертификата

сертификат пользователя

сертификат хоста

Имя   
Английскими буквами, например: Ivan

Фамилия   
Английскими буквами, например: Ivanov

Common Name (CN)   
CN пользователя английскими буквами, например: Ivan Ivanov

E-mail   
Электронный адрес может содержать английские буквы, цифры, дефис, точку и @

Телефон   
Допускаются цифры, дефисы и пробелы. Например: 495 123-45-67 или 1234567

Организация   
Выберите организацию из списка

Пароль

Повторите пароль   
Длина пароля - не менее 8 символов, должна быть хотя бы одна буква и хотя бы одна цифра

Отправить заявку в удостоверяющий центр:

Создать заявку      Проверить сертификат      Закреть



# Example of the interactive mode

```
Администратор: C:\Windows\System32\cmd.exe - certreq.exe
Would you like to generate a new certificate request ([y]es/[n]o)?y
Certificate type ([h]lost/[u]lser): u
> User certificate selected
1. Your name (Name Surname): Ivan Ivanov
2. Common Name - CN (Define CN only if it differs from your name. Otherwise leave blank and press Enter): Ivan Ivanov
3. Select a number of your organization from the following list:
1  RRC KI, grid.kiae.ru
2  SINP MSU, sinp.msu.ru
3  JINR, jinr.ru
4  PNPI, pnpi.nw.ru
5  SGU, sgu.ru
6  ICMM RAS, icmm.ru
7  KazNC RAS, knc.ru
8  SPII RAS, spiiras.nw.ru
9  CC FEB RAS, febras.net
10 IPCP RAS, icp.ac.ru
11 NIIR, niir.ru
12 SFU KRAS, sfu-kras.ru
13 URIIT, uriit.ru
14 ICT SBRAS, sbras.ru
15 BINP, inp.nsk.su
16 SPbSTU, spbstu.ru
17 IFMO, ifmo.ru
18 IMM RAS, inet.ac.ru
19 NTCSTM, ntcstm.troitsk.ru
Number of your organization: 2
> Selected Organization Unit: sinp.msu.ru
4. Your email address (youremail@domain.com): iivanov@sinp.msu.ru
5. Your phone number (+7 495 123-45-67): +7 495 123-45-67
6. Password.
Enter password:
Repeat password:
> Data fields and values:
> 1. User name: Ivan Ivanov
> 2. CN: Ivan Ivanov
> 3. Organization Unit: sinp.msu.ru
> 4. Email: iivanov@sinp.msu.ru
> 5. Phone: +7 495 123-45-67
> 6. Password is not empty.
>
To change any data value type the number of the data field (e.g. 4 for email) and press <ENTER>. If all data values are correct just press <ENTER>.
```

# 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\*\*\*](http://www.ngrid.ru))
- Certreq is written on python language ([\*\*\*www.python.org\*\*\*](http://www.python.org))
- OpenSSL library is included in the program distribution ([\*\*\*www.openssl.org\*\*\*](http://www.openssl.org))
- py2exe was used to prepare certreq.exe file for Windows ([\*\*\*www.py2exe.org\*\*\*](http://www.py2exe.org))

# Alternative solution

- Certificate authority with highly functional web-interface. As an example of such a CA OpenCA project ([www.openca.org](http://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?