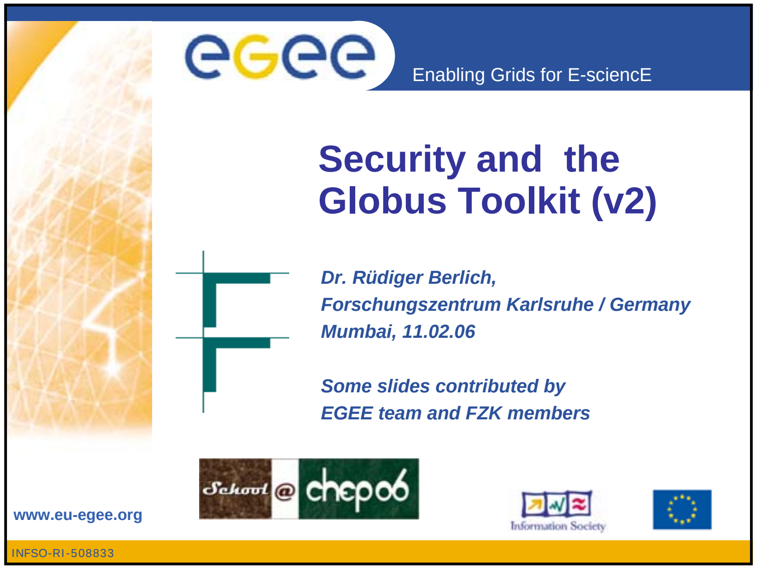


Enabling Grids for E-sciencE

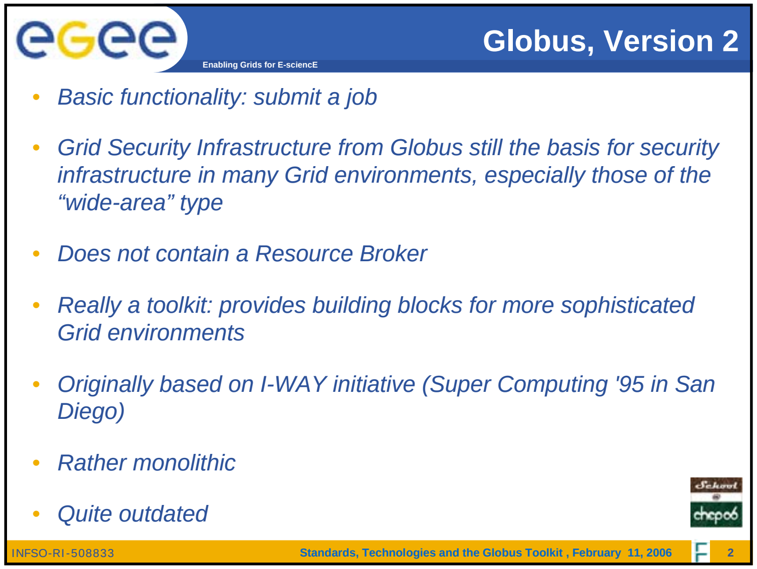
Security and the Globus Toolkit (v2)

Dr. Rüdiger Berlich,
Forschungszentrum Karlsruhe / Germany
Mumbai, 11.02.06

Some slides contributed by
EGEE team and FZK members

www.eu-egee.org

INFSO-RI-508833

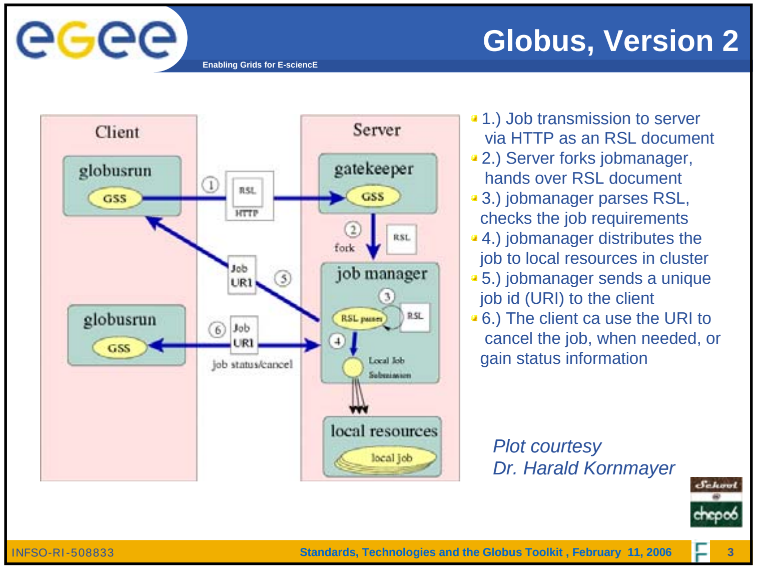


Enabling Grids for E-sciencE

Globus, Version 2

- *Basic functionality: submit a job*
- *Grid Security Infrastructure from Globus still the basis for security infrastructure in many Grid environments, especially those of the “wide-area” type*
- *Does not contain a Resource Broker*
- *Really a toolkit: provides building blocks for more sophisticated Grid environments*
- *Originally based on I-WAY initiative (Super Computing '95 in San Diego)*
- *Rather monolithic*
- *Quite outdated*

INFSO-RI-508833 Standards, Technologies and the Globus Toolkit , February 11, 2006 2



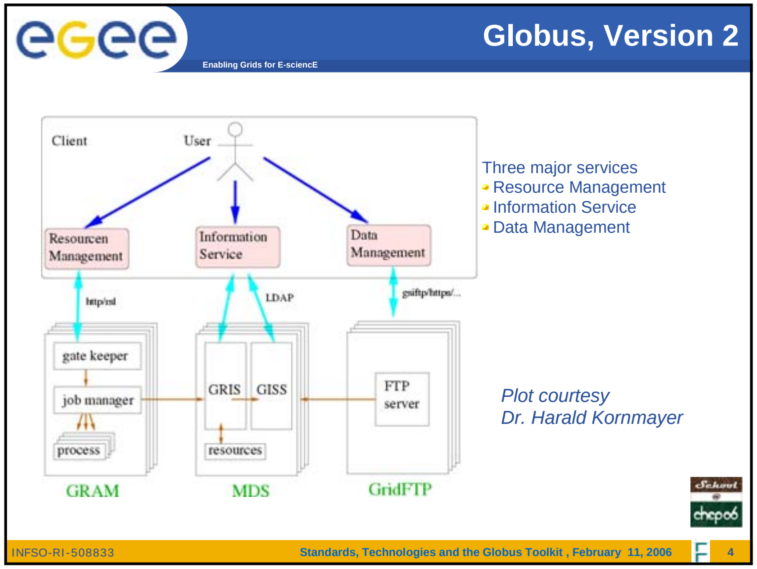
Enabling Grids for E-sciencE

Globus, Version 2

- 1.) Job transmission to server via HTTP as an RSL document
- 2.) Server forks jobmanager, hands over RSL document
- 3.) jobmanager parses RSL, checks the job requirements
- 4.) jobmanager distributes the job to local resources in cluster
- 5.) jobmanager sends a unique job id (URI) to the client
- 6.) The client ca use the URI to cancel the job, when needed, or gain status information

Plot courtesy
Dr. Harald Kornmayer

INFSO-RI-508833 Standards, Technologies and the Globus Toolkit , February 11, 2006 3



Enabling Grids for E-sciencE

Globus, Version 2

Three major services
- Resource Management
- Information Service
- Data Management

Plot courtesy
Dr. Harald Kornmayer

INFSO-RI-508833 Standards, Technologies and the Globus Toolkit , February 11, 2006 4

Grid Security and Certificate Authorities

Enabling Grids for E-sciencE

- **Public / private key infrastructure**
- **Authentication and Authorisation based on X509 certificates**
- **Certificate authority hands out keys to users who have proven their identity.**
- **Trust relationships between CAs allow for “chains of trust”.**
- **Revocation lists to handle expired or compromised certificates**

PKI example bank / customer

Enabling Grids for E-sciencE

- **Customer writes mail to bank, wants privacy**
- **Customer encrypts message with the bank's public key and signs the encrypted text**
  - create checksum of text
  - encrypt checksum with his private key
- **Upon receipt, bank checks validity of message**
  - calculates checksum
  - encrypts customer's checksum with his public key
  - compares both values
- **Bank decrypts message with its own private key**
- **This procedure is only as secure as the private keys !!!**

Grid Security and Certificate Authorities

Enabling Grids for E-sciencE

Globus X509 Zertifikate

- Authentication
- Private key
- certificate
  - *Public key*
  - *Information*
- Request File

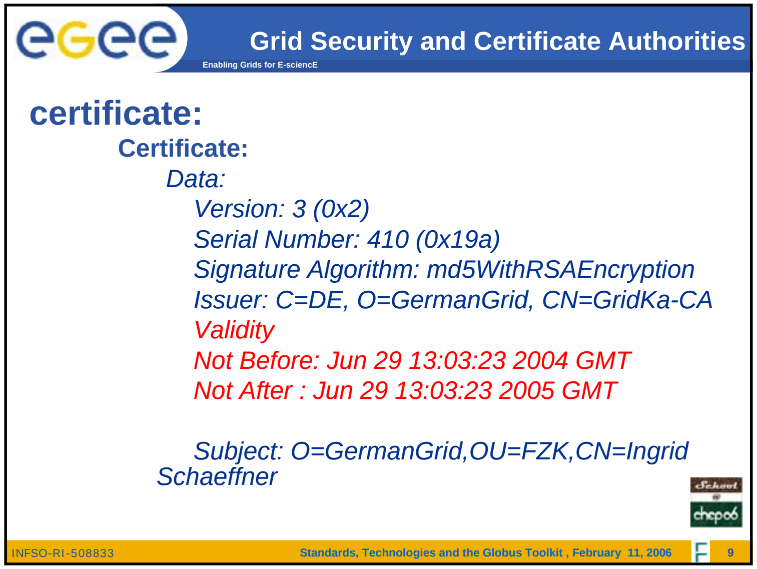
Grid Security and Certificate Authorities

Enabling Grids for E-sciencE

Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,905F37A0F89EC9CB

jUtSpSgEFVGMORBPzEMcnHRNI4d11CY+y+h5xZ8Swp2OA+R1cmAUhPT3AFqYP6Fa
5JJBADo7Bh3rCsq2Y04xmwtBpKhq6CgMuGZoynLarCUXfa+Jv2xBHXGbCBjVYnFu
YBLvCgv87YYQs+UJsQrTgz70lbpVcnMRr/qlCDcP7Z1xxRZkkGaqIm1V/7KlpaM0
lh5bnkKE18bNeMfrIipBkQGrIG7bOJhZ5qWeBVOJuiGe3drBUIx1SHXp5czvj6Ec
UYd06nKGbmuYAtBiZna2/aN04pnIRoycb/K4wOyGnm/EYJqqPv98rD4j+uxQLZyq
U7ozMioSNHB3E5buNfMEVlyyjR+3Ua5iW1JB7C/AfW3kTh+dljisfJAccoEHz44G
2gMtdwdtiFoqRyXkzoafEssOjK5urxOjDbJqb8GGWZKqsyIIg4o6P+bMsGL9qSe5
R51yA9L4YQZ2TCJpZ2lIaoe5BNjildZr96lpILr85aaiP1GyFC59+AHfN8vUytCi
hLApUlYmGW6eP1BQnP5U1UaDreYbi5vN2C74HMOxQML9/fEgNuL06O9Rt8LlUoMe
Y6kZfKb5pd8ERmnRazgJZ4zrib5sAkDZwdfl/BFhSwbvzr6WxxAPTLGDlPmZulj0
A0HvAJ8MIrKCx9oWA4uhbooeaNmfeinF6jBN2kLXGotH2I/5vxjZSw/hzNOmnnkD
QeHqIwZCD1NFM7IrnBBkJLKmC4985pgW8w6D0N3EHV4=
-----END RSA PRIVATE KEY-----
```



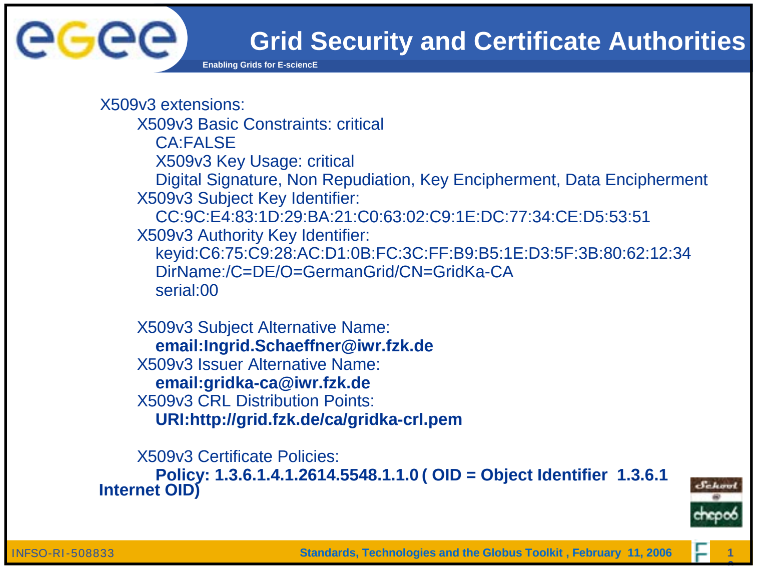
Grid Security and Certificate Authorities

Enabling Grids for E-sciencE

certificate:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 410 (0x19a)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=DE, O=GermanGrid, CN=GridKa-CA
        Validity
        Not Before: Jun 29 13:03:23 2004 GMT
        Not After : Jun 29 13:03:23 2005 GMT

        Subject: O=GermanGrid,OU=FZK,CN=Ingrid
    Schaeffner
```



Grid Security and Certificate Authorities

Enabling Grids for E-sciencE

```
X509v3 extensions:
    X509v3 Basic Constraints: critical
        CA:FALSE
        X509v3 Key Usage: critical
        Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
    X509v3 Subject Key Identifier:
        CC:9C:E4:83:1D:29:BA:21:C0:63:02:C9:1E:DC:77:34:CE:D5:53:51
    X509v3 Authority Key Identifier:
        keyid:C6:75:C9:28:AC:D1:0B:FC:3C:FF:B9:B5:1E:D3:5F:3B:80:62:12:34
        DirName:/C=DE/O=GermanGrid/CN=GridKa-CA
        serial:00

    X509v3 Subject Alternative Name:
        email:Ingrid.Schaeffner@iwr.fzk.de
    X509v3 Issuer Alternative Name:
        email:gridka-ca@iwr.fzk.de
    X509v3 CRL Distribution Points:
        URI:http://grid.fzk.de/ca/gridka-crl.pem

    X509v3 Certificate Policies:
        Policy: 1.3.6.1.4.1.2614.5548.1.1.0 ( OID = Object Identifier  1.3.6.1
Internet OID)
```