SDG CA Updates

APGrid PMA meeting, Nov. 29, 2005

Morrise Xu (morrise@cnic.ac.cn)
NTARL, CNIC, China

Outline

- **Introduction to SDG and SDG CA**
- **Current status of SDG CA**
  - **Number of issued certificates**
  - **Subscribers**
- **Details of CA operation**
  - **Staff**
  - **hardware / equipments / facilities / physical access**
  - **events recorded and archives**
- **detailed flow for issuing certificates**

CNIC: Computer Network Information Center

- Institute of CAS
- Include 6 Departments
  - CNNIC
  - CSTNet Network Center
  - Supercomputing Center
  - Scientific Database Center
  - Academic Resource Planning Center
  - Network Technology and Applications Research laboratory
- 352 Staff + 154 Graduate Students

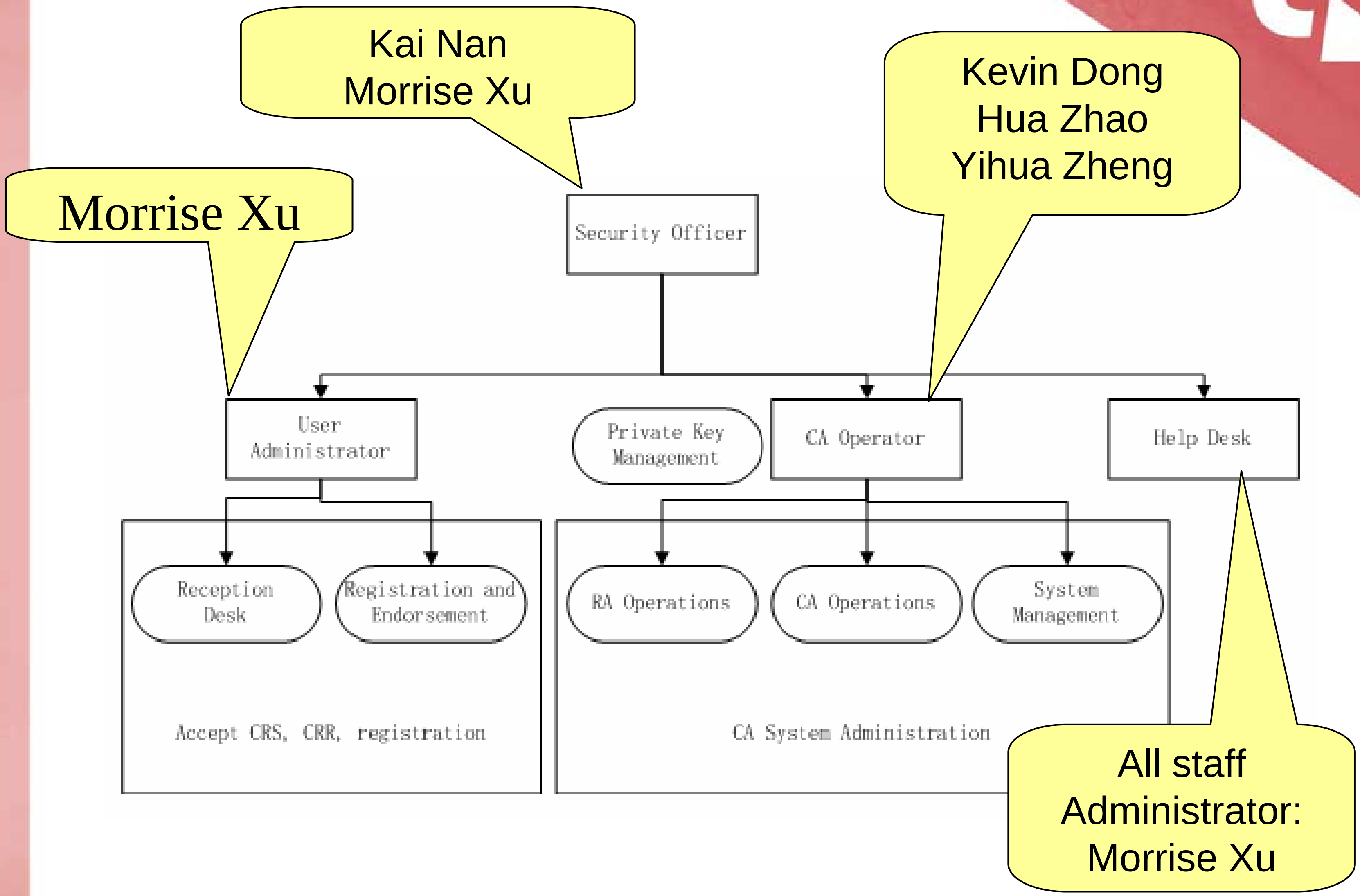
SDG and SDG CA

- **Scientific Data Grid (SDG)**
  - Scientific Data Grid (SDG) is an application grid based on scientific data resources sharing and collaboration.
  - System platform
  - SDG Middleware
  - Security system
  - Application system
- **SDG CA**
  - the SDG security infrastructure
- **SDG CA CP/CPS**
  - http://www.apgridpma.org/meetings/200511/SDG-CA-CP-CPS-eng.pdf

Current status of SDG CA

- **Number of issued certificates**
  - **121 certificates**
    - 87 valid certificates
      - 4 host certificates
      - 83 user certificates
    - 34 revoked certificates
      - 1 host certificate
      - 33 user certificates
- **Subscribers**
  - **SDG members**
    - 45 institutes of CAS
  - **CNIC staff**
  - **SDG PMA**

Details of CA operation – staff



Details of CA operation – hardware / equipments / facilities / physical access –

- **CA server**
  - Dell 1U rack server, Red Hat Linux AS3
  - Offline, no connection to any other network
  - UPS is supplied
- **RA server**
  - Dell 1U rack server, Red Hat Linux AS3
  - connected to the Internet
    - Only the necessary ports for RA operation are opened. Other ports are filtered by the firewall.
  - UPS is supplied
- **Web server (repository)**
  - The same machine as RA Server
  - connected to the Internet
    - Same as RA Server
  - UPS is supplied

Details of CA operation – hardware / equipments / facilities physical access – (cont'd)

- **CA room**
  - Located in the CNIC machine room.
  - Limited person can enter.
    - Security Officer
    - CA Operators
    - Other CNIC administrators
  - Doors equipped with fingerprint recognition system.
  - Monitored by the CCTV
- **Physical access**
  - The CA operator is not allowed to access the CA machines alone and need to do so with the other CA operator.
  - If the CA operator needs to access the CA machines alone, he must notify the fact to the user administrator by Emails before and after entering the room.
  - All events about the access to the machines must be recorded in the paper sheets prepared in the room. The events include the names of CA operators, date and time of entering/leaving the room, and the purpose of the access to the machine.
  - The filled sheets will be kept in the dedicated safe box.

Details of CA operation – events recorded and archives –

- **CA system logs**
  - Access and operation logs to the CA daemon process
  - Error logs for accesses and operations to the CA daemon process
  - Operation logs of the CA daemon process
- **RA system logs**
  - Access and operation logs to the RA daemon process
  - Error logs for accesses and operations to the RA daemon process
  - Logs of issued certificates
  - All issued CRLs
  - The date of issuance of CRLs
  - All CSRs and CRRs
- **Linux system logs**
  - shutdown/boot/reboot logs of the CA server and the RA server
  - login/logout/sudo logs of the CA and the RA server
  - other logs archived by Linux operation of the CA and the RA server
    - secure/cronlog/maillog/messages(sulog)syslog/errorlog

Details of CA operation – events recorded and archives – (cont'd)

- **Logs of physical access to CA machines**
  - Paper sheets which record all events about the access to the CA room.
- **Emails**
  - All emails received by the SDG CA
  - All emails of system-logs sent from the RA server
- **Other documents**
  - A list of email addresses of end entities
  - All issued certificates
  - for each approved request, how the request was approved
  - for each rejected request, how the request was rejected
  - official documents if they are used for identification of entities
  - All versions of the CP/CPS
  - All versions of the Certificate and CRL Profile
  - All Audit reports

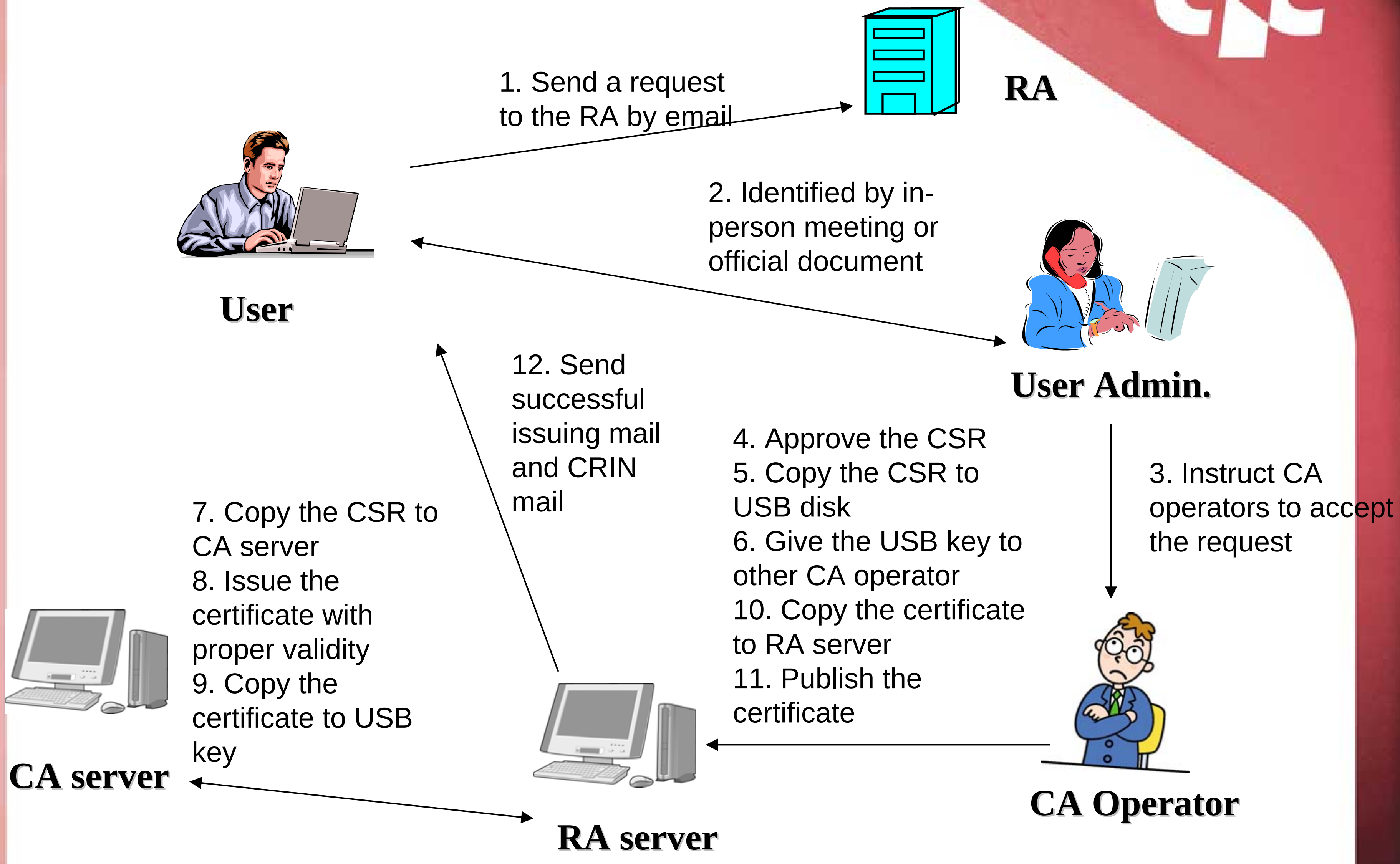
Detailed flow for issuing certificates

- **End entities request certificates**
  - Register and fill the Certificate Signing Request
  - Send the request to RA (post in website)
- **User Administrator check the requests**
  - Identified by the in-person meeting or official document
  - Accept the request or not
  - Notify the RA operator
    - Send the secure email to the RA operator or
    - Tell the RA operator directly(Log the event)
- **RA operator approved the requests**
  - CA operators (including RA operators) go to the CA Room
  - RA operators check the CSR (DN,Organization Name, Certficate Role etc.)
  - RA operators approve the requests after the notification
- **RA operator transfer the requests to CA operator**
  - RA operators zip the CSRs
  - RA operators copy the CSRs to the USB key
  - CA operators copy the files into the CA machine with USB key
  - CA operators unzip the CSRs

Detailed flow of issuing certificates– (cont'd)

- **CA operator - issue certificates**
  - CA operators issue the certificates with proper validity
- **CA operator - transfer the certificates to RA operator**
  - CA operators zip the certificates
  - CA operators copy the certificates to the USB key
  - RA operators copy the files into the CA machine with USB key
  - RA operators unzip the certificates
- **RA operator - publish the certificates**
  - RA operators publish the certificates to the website
  - Auto sending the success mails and CRIN mails

Detailed flow of issuing certificates– (cont'd)



Detailed flow of issuing certificates– (cont'd)

- **For revoking the certificates, most of the operations are the same as issuing certificates except:**
- **End entities request certificates revocation**
  - Fill the form with CRIN or signature or sending the official document to User Administrator
- **CA operators issue the Certificate Revocation Requests**
  - CA operators issue the CRRs
  - CA operators issue the Certificate Revocation List
- **RA operator publish the CRL**
  - RA operators publish the CRL to the website

Thanks!