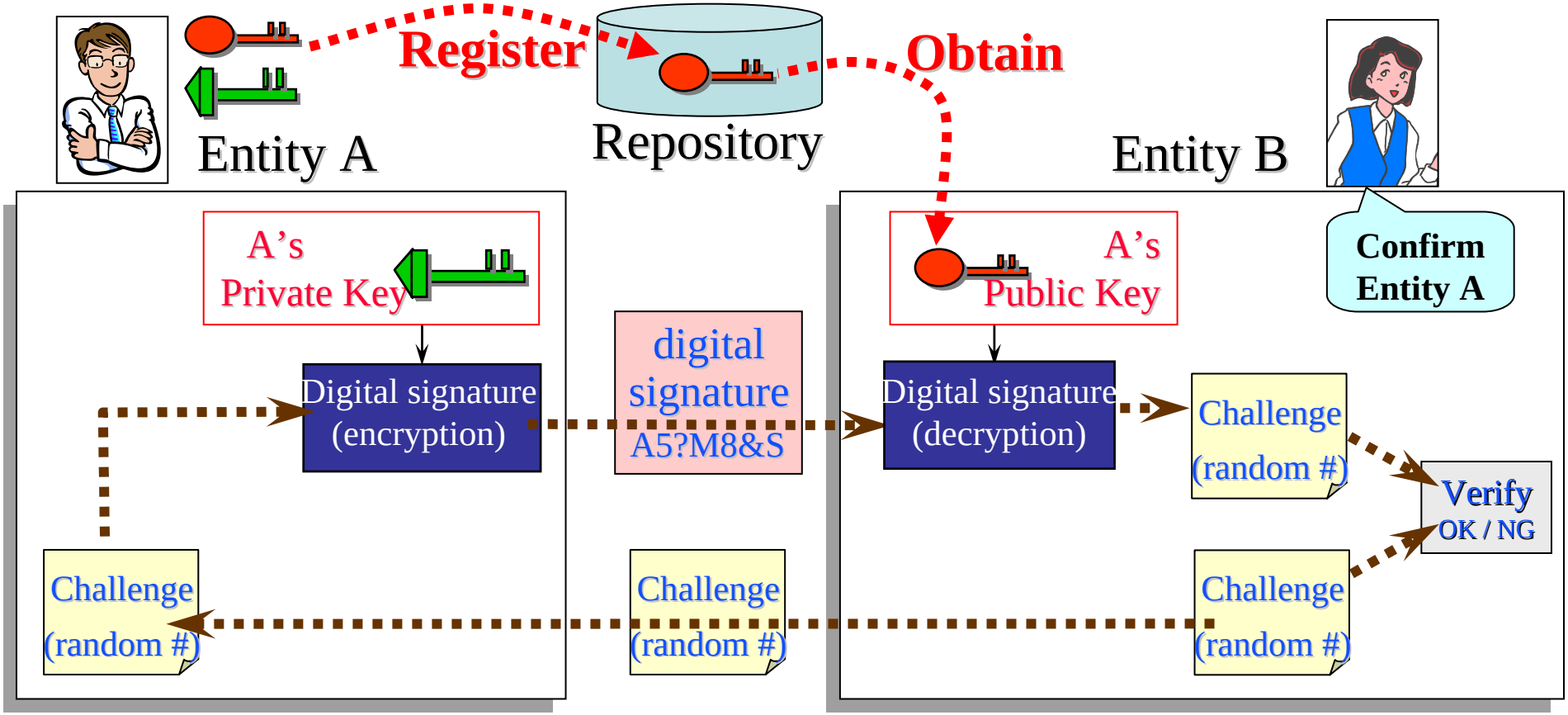
Some thoughts on issuing Web server certificates

APGrid PMA meeting, Nov. 29, 2005

Yoshio Tanaka (yoshio.tanaka@aist.go.jp)
Grid Technology Research Center,
AIST, Japan

Review PKI



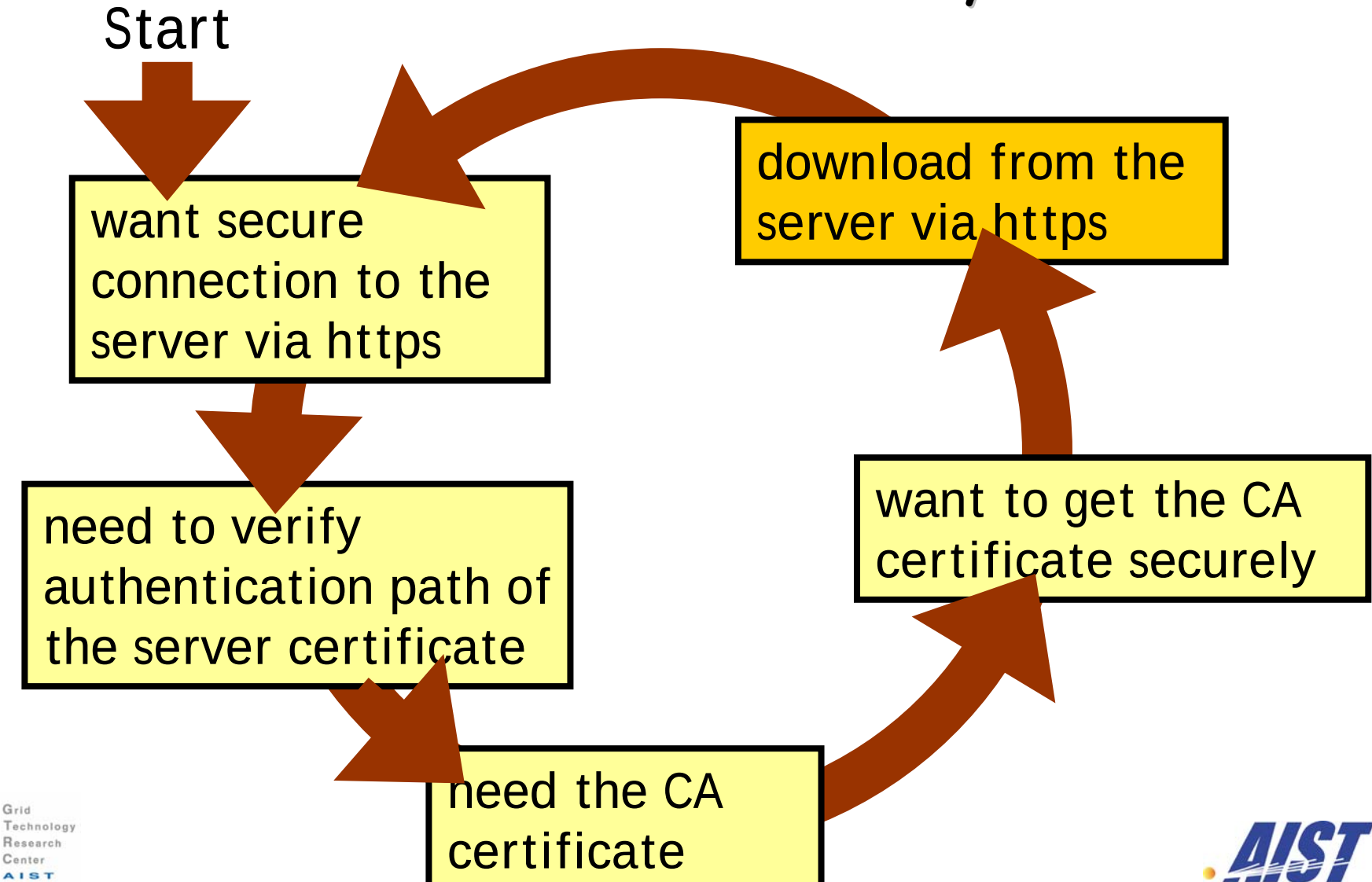
- **How entity B verifies whether A's public key is the real one?**
  - Use Public Key Certificates issued by trusted third party (CA)

Public Key Cert. and CA

- **Public Key Certificates guarantees**
  - integrity of the public key
  - identification of the certificate holder
- **Prevent man-in-the-middle attack**
- **CA must be**
  - a trusted authority
  - operated appropriately (securely)
- **Public Key Certificate is signed by CA private key**
  - It is verified using CA public key
- **How do you obtain CA public key?**
  - CA public key must be published in trustworthy method.
    - https?

Chicken-egg problem

- **Suppose CA public key (CA cert.) is published by https whose web server certificate is issued by the CA**



The other problem if CA cert. is imported into the browser

- **An application (domain) has its own repository of trusted CAs.**
  - e.g. Windows IE CA repository, Globus /etc/grid-security/certificates/
  - Certificates issued by the trusted CAs will be trusted
  - Certificates issued by CAs which are not in the repository will not be trusted and give you a warning

  - If the CA is once imported into the repository, you will never see warning unless the CA cert is expired or used for different name.

What is the problem?

- **Again, an application (domain) has its own repository of trusted CAs.**
  - Browser is used for E-commerce
    - handles real money
  - Grid (globus) client is used for computation and data access
    - your access may be accounted, but no direct paying of real money
  - All CAs in a repository must have be in the same level
  - If your CA is imported into the browser and if your CA is compromised
    - Evil person may build an E-commerce site whose web server certificate is issued by your CA
  - Our CAs are for Grid authentication, not for wide-range of authentication
    - We cannot operate our CA with the same level of commercial CAs