JPNIC Certification Authority Overview

Japan Network Information Center

Taiji Kimura

Topics

- Why JPNIC is planning CA
- Status in JPNIC CA project
- Certificate management model
- Future directions

Why JPNIC is planning CA

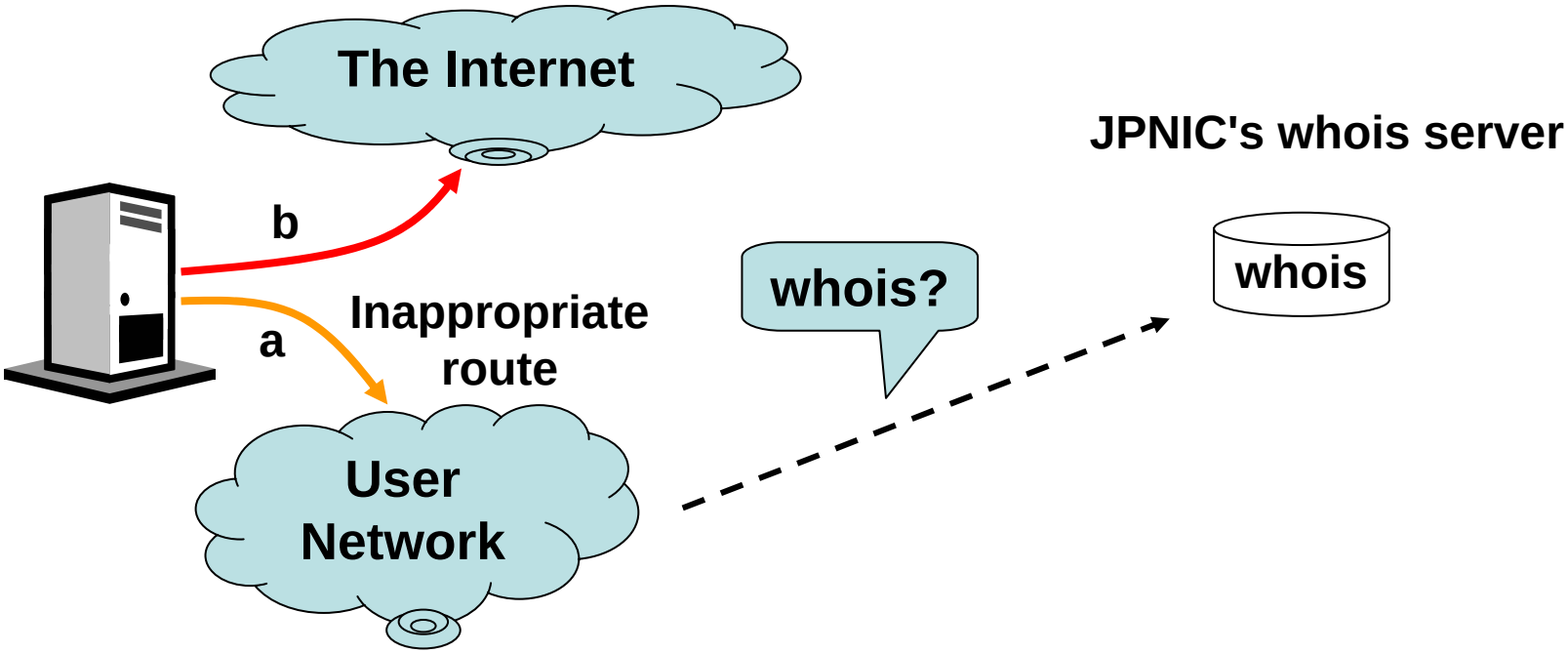
Critical threats and IP address blocks

- IP address hijacking and malformed routing information
  - They can bring untraceable attacks.
    - e.g. DoS or Spam

- When these threats happened, legitimate information on IP address block is needed.

Threats and whois

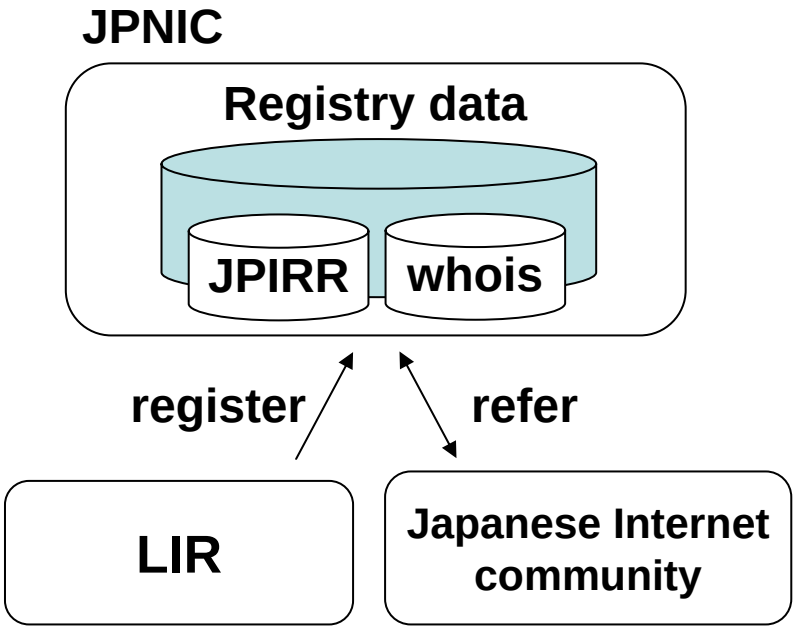
- If IP address(es) or routing information is hijacked we can lookup whois database for responding these problems.



"registry data" in registries

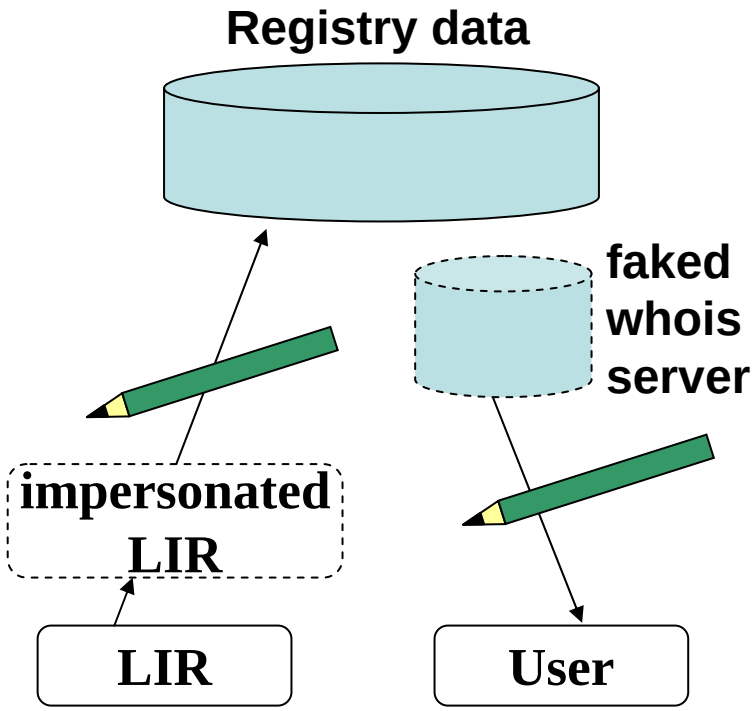
- Allocation and assignment information
  - They also have
    - LIR's information
    - Network information
    - AS information
    - Contacts

  etc.



Threats against whois

- When "whois hijacking" can happen…
  where should we lookup?



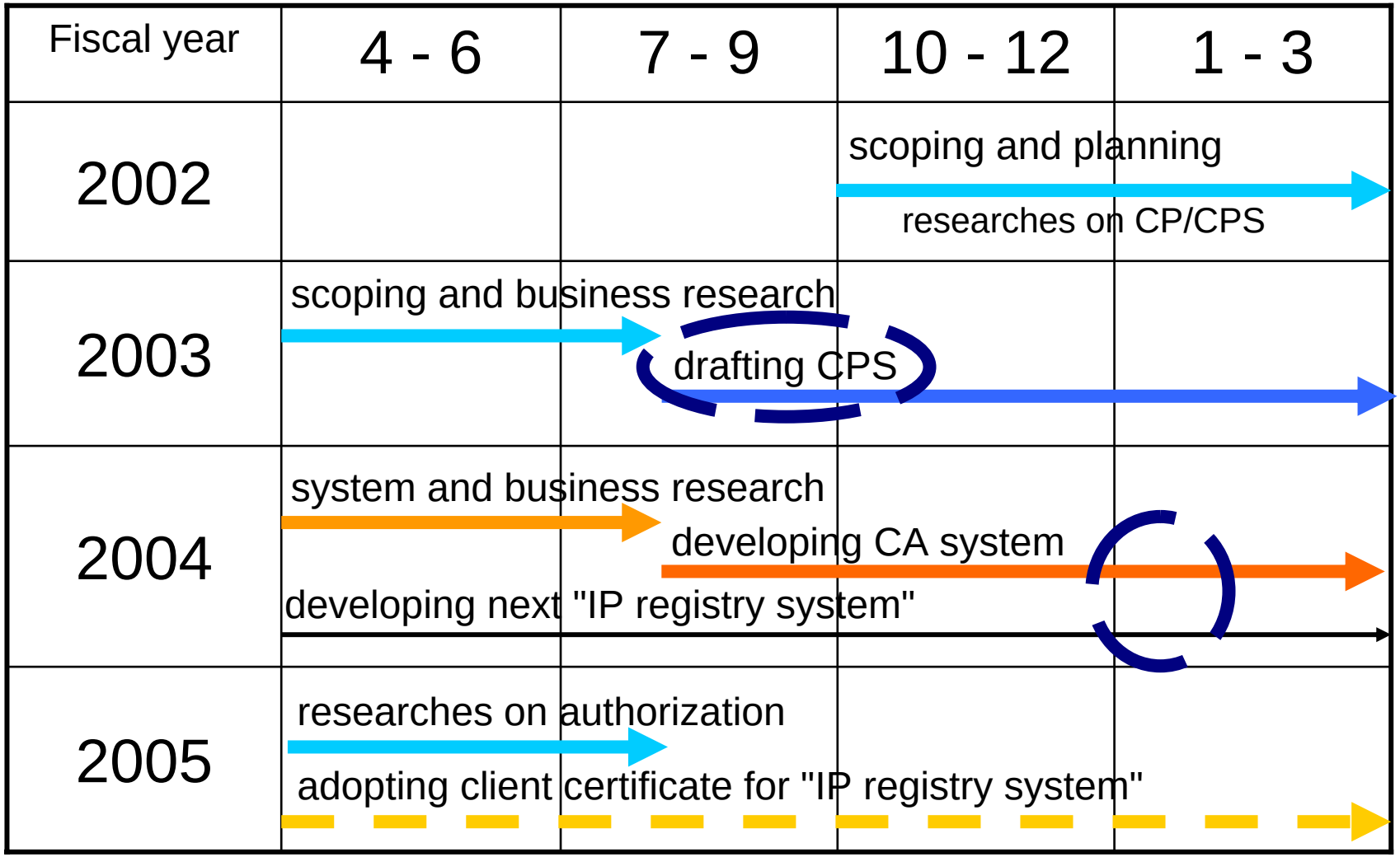
Our actions against the threats

- Building secure operations on registry data
  - registrations and modifications
  - providing reference for legitimate registry data

JPNIC CA's goal
- Strong authentication in "IP registry system"
- Test-bed for certificates based on registry data
  e.g. Verification of assignment

Status in JPNIC CA project

Status in JPNIC CA project



Drafting CPS (Certification Practice Statement) for JPNIC CA

- Our objectives
  - This is for clarifying our authentication process.
    - We can revise processes.
    - Users can find almost security level.
  - Our registration procedure for LIR will have effects to future usage of certificates.
- Status
  - New version is being drafted after the first draft in 2003 (along with RFC3779).
    - According to installed facilities, scale of management staff are adjusted. This became more specific from the previous draft.
    - The document will be released March 2004.

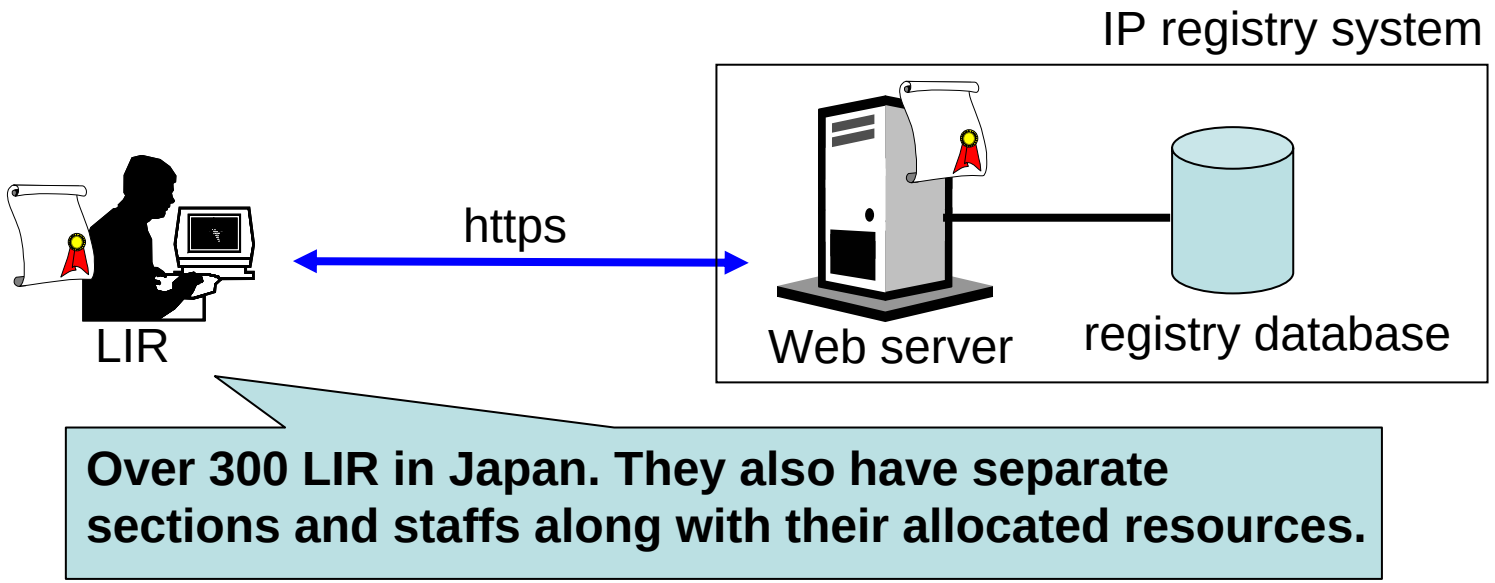
Developing CA system

- For realizing LIR's registration procedure.
- We designed to collaborate with new "IP registry system" (ongoing project).
  - Defining relationships between users, maintainers and resources along with Japanese LIR's situation.
- Testing CA system and "IP registry system"
  - The CA system have already set up and tested independently. Both system will be ready after this collaborative tests.
  - Client certificate will be applied this year.

Certificate management model

Client certificates for authentication

- How should we manage client certificates?

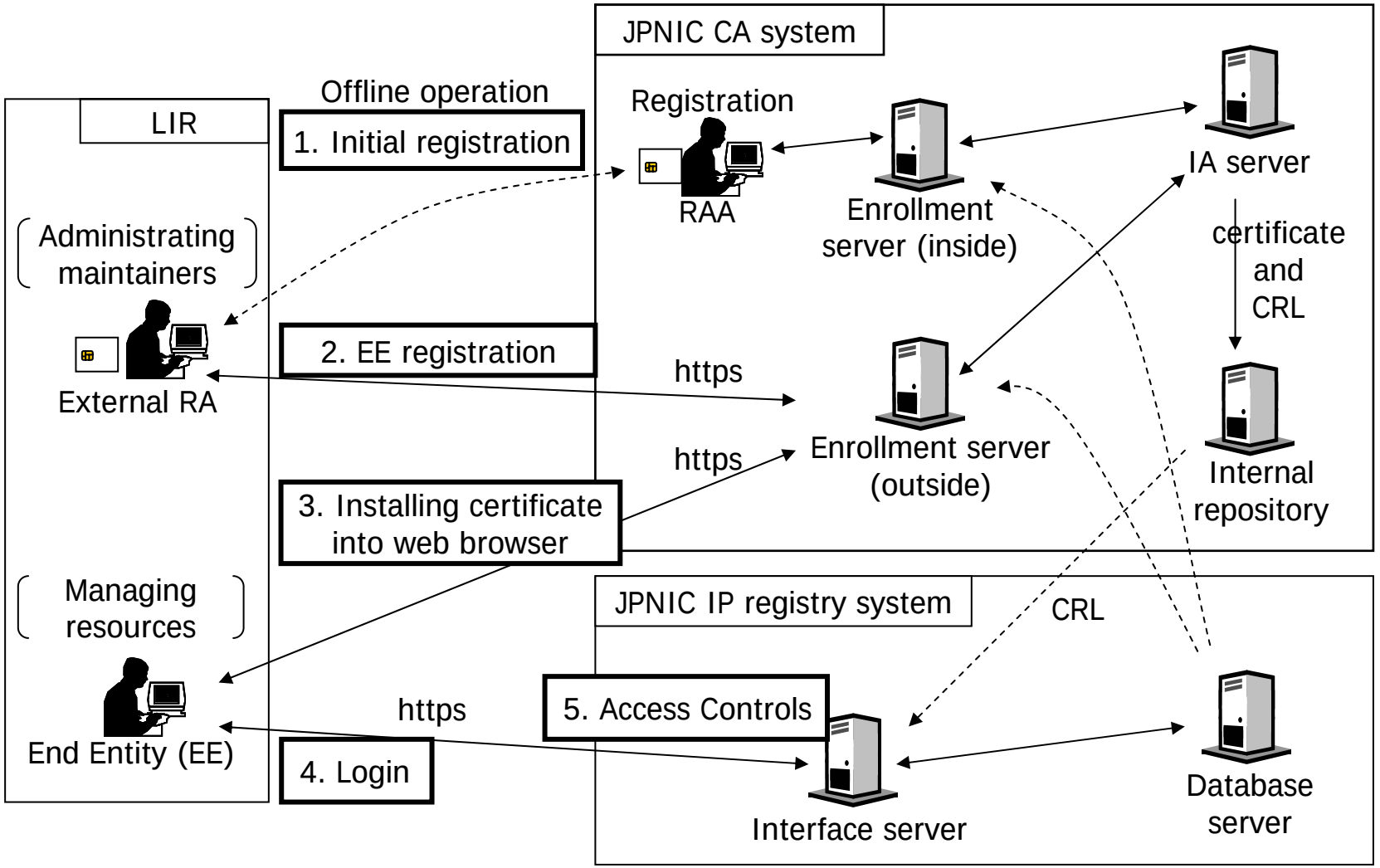


• It's hard to check their identities and roles in all LIR.
• It's hard to support all users they have NIC-handles (There are huge amount of handles in our database.)

Entities in our model

- External RA (in LIR)
  - Having right to manage EE for their LIR
  - Not having right to submit request for resource allocation and reporting assignment.
- EE - End Entity (in LIR)
  - Having right to submit request for allocation and assignment.
- RAA - RA Authority (in JPNIC)
  - RA for registering external RA in LIR
- Enrollment server
  - Used by external RA and RAA for requesting certificates and revocations.
- IA server - Issuing Authority server
  - Checks request from RA or RAA and issue certificate or CRL
  - Managed with secure manner

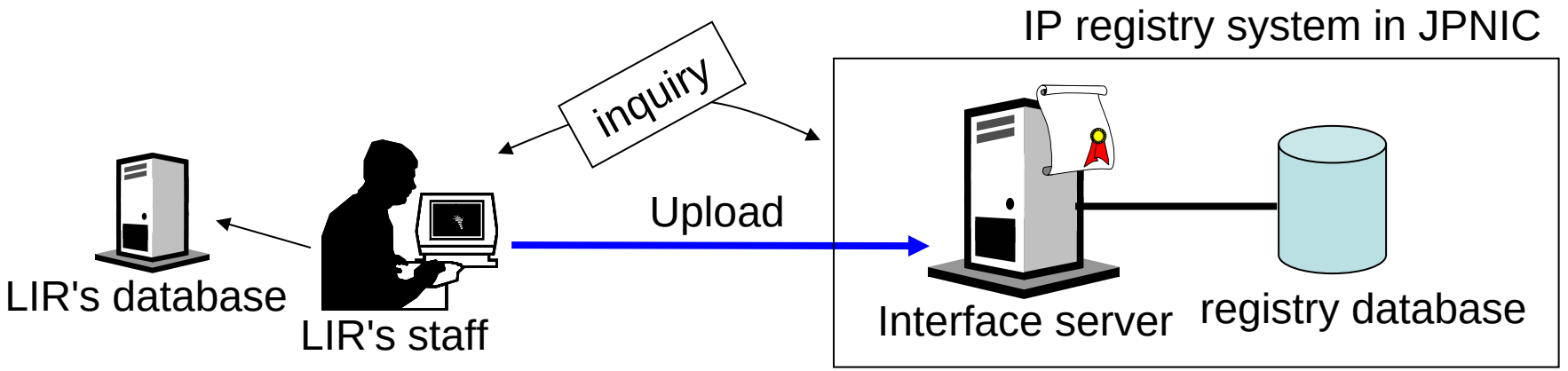
Certificate management model



Future directions

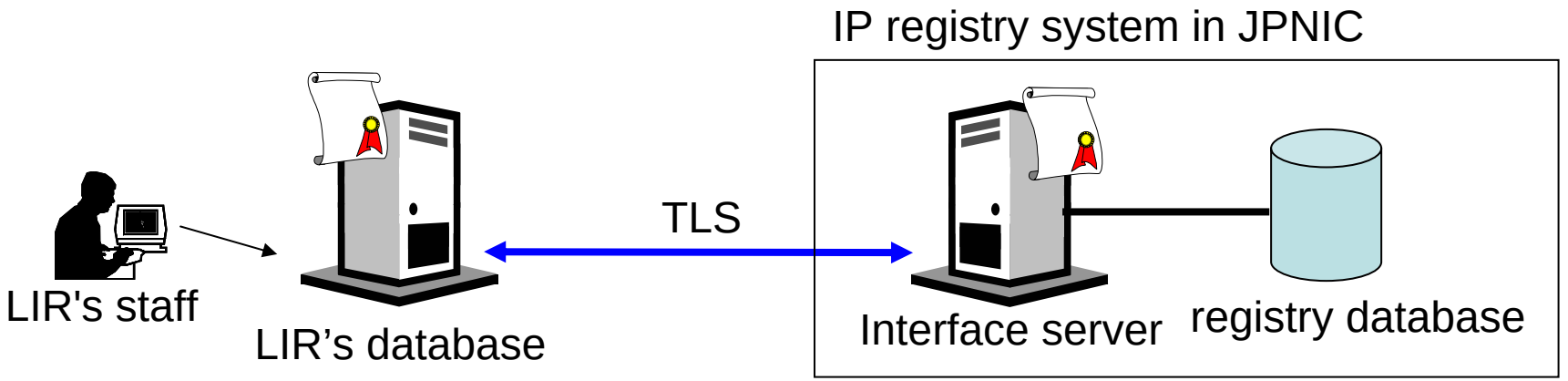
Certificates for web transactions(1/2)

- Transactions between LIR and JPNIC
  - Sometimes huge amount of allocation and assignment information is needed to transfer.
  - We have to wait until enough data is transferred correctly.



Certificates for web transactions(2/2)

- Web transactions using TLS
  - Transferring data object effectively
  - Semi-automated judging procedure
    - for shorter response time



Authorization using RFC3779

- Authorization of use of address resources
  - X.509 Extensions for IP Addresses and AS Identifiers, RFC3779
  - JPNIC CA system is able to issue certificates with the extensions.
    - Management and validity of certificates will be discussed in the future.

Certificate for JPIRR

- Client authentication
  - Strong authentication for IRR system
    - Web interface
  - This certificate may also be used for digital signature.
    - IRR's mirroring model

Summary

- JPNIC is planning CA for
  - Client authenticate with IP registry system
  - Test-bed for use of registry data
- Status in JPNIC CA project
  - Our CA system is now taking collaborating test and CPS is being revised
- Certificate management model
  - LIR's RA registers EE for client certificate.
- Future directions
  - Web transactions

Questions?