A Study of Certification Authority Integration Model in a PKI Trust Federation on Distributed Infrastructures for Academic Research

International Symposium on Grids & Clouds 2016
15 March 2016
Academia Sinica, Taipei, Taiwan

Eisaku SAKANE, Takeshi NISHIMURA, Kento AIDA

National Institute of Informatics, Japan

National Institute of Informatics

Outline

- Introduction
- Objects and Issues
  - Typical CA Architecture
- Proposals
- Discussions
- Related Works
- Summary

National Institute of Informatics

Introduction

- Background
  - Among certification authorities (CAs) in an academic PKI trust federation, most of academic organizations that operate CA install by themselves the CA equipment in their building.
  - It is necessary to maintain such CA equipment and to obtain the special operators.
  - Consequently, the high cost of CA operation weighs heavily on the CA organization.
  - For research institutes whose essential duties are not the CA operation, the burden on the high cost of CA operation is an earnest problem, and cost reduction with increasing the efficiency of the operation is an important issue.

Introduction (cont'd)

- Guiding question
  - How about trying for more than one operating organization to reduce cost operations?
- Importance of the research
  - We propose a method of increasing the efficiency of CA operations in cooperation between more than one CA operating organization.

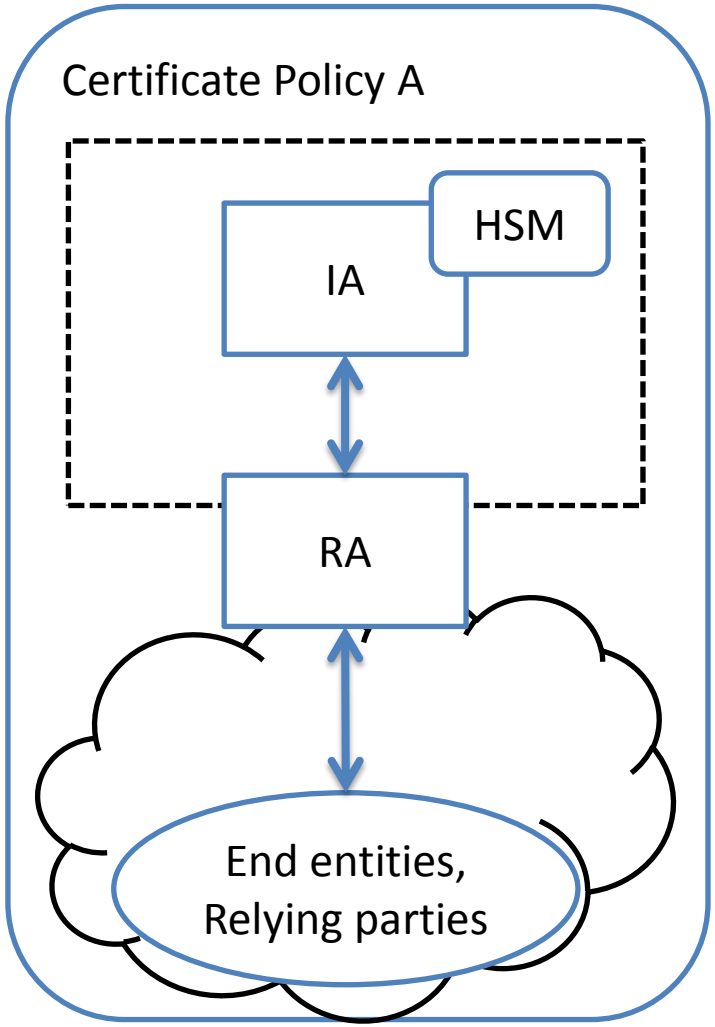
Premise of the Argument

- We do not discuss how to build from scratch a CA that covers each research community.
  - Keep the independence of CA operating organization.
- We do not discuss the following:
  - Two CA operating organizations outsource CA to a commercial CA vendor and share the expenses.
- We discuss how to integrate existing CAs without being forced to a drastic change in order to reduce the cost of the CA operations.
  - From user's point of view, CA service procedures for users should be unchanged as possible.
  - From operator's point of view, the changes of CA operation procedures should be small if possible.

National Institute of Informatics

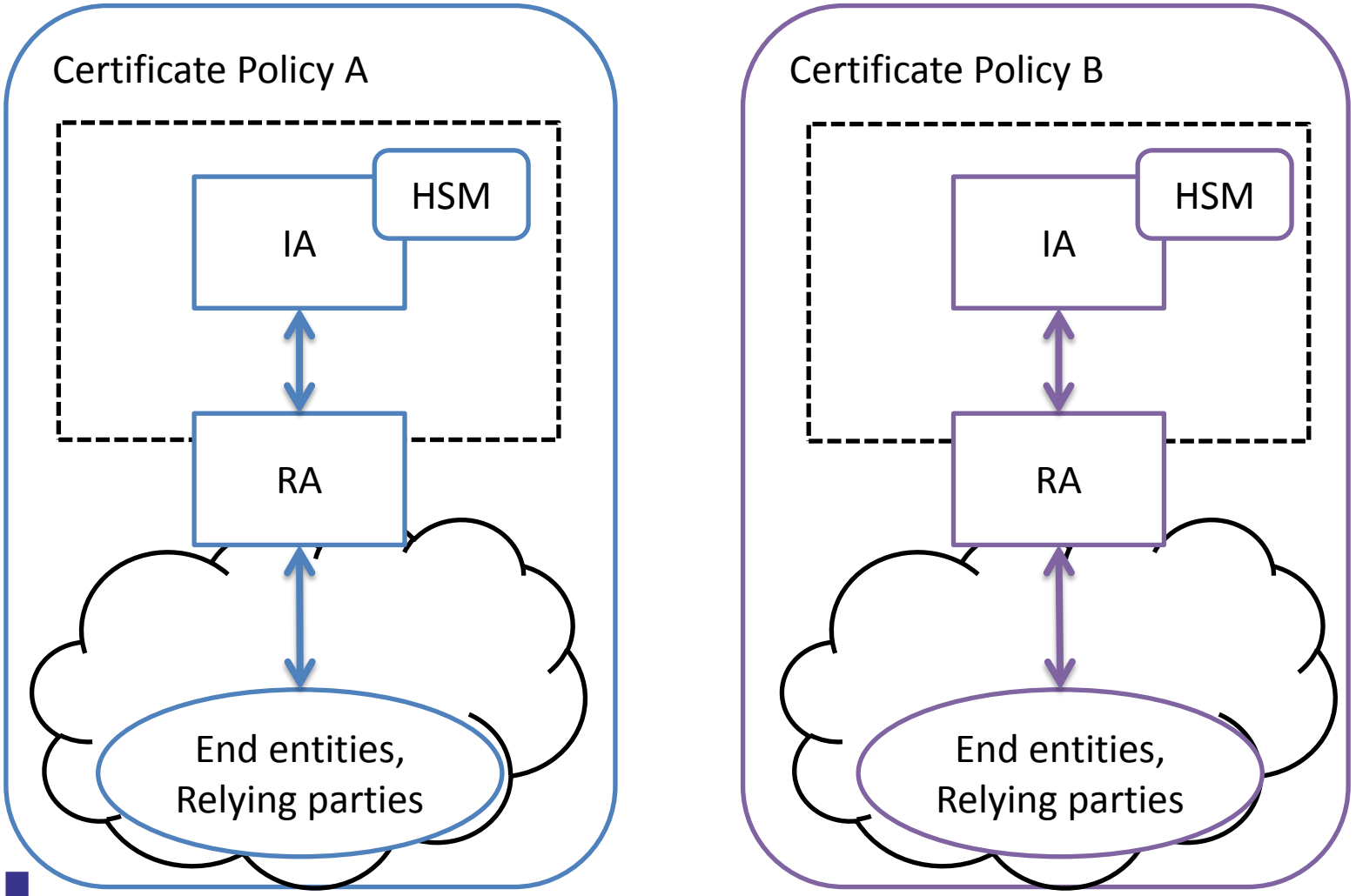
Typical CA Architecture

- CA architecture in question
  - Composed of IA and RA servers
  - IA located in a private network connects only the RA and is a dedicate machine for only signing operations.
  - RA connected to the public network receives the request from end-entities and conveys it to the IA.



National Institute of Informatics

Typical CA Architecture (cont'd)



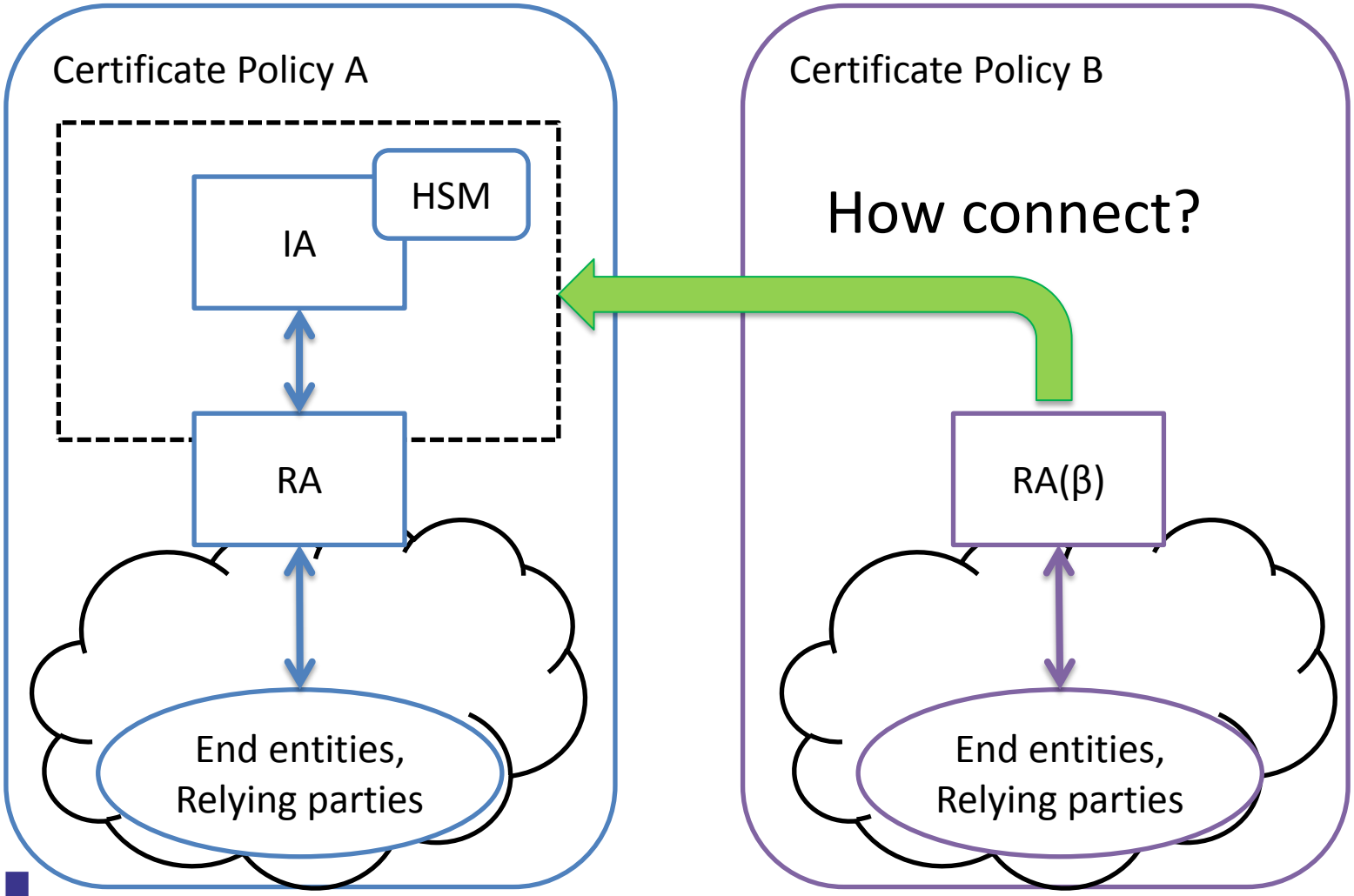
Basic Idea

- Interference in certificate policies would be kept down to a minimum if each RA is independently operated as before.
  - The research community should have the responsibility to vet user identities.
  - It is difficult for one RA to vet user identities in the other community because RA operations are heavy duties.
- Issuing operations are the following:
  - Strictly management of the CA private key
  - Response to the requests from the RA
- It would be unnecessary to operate the IA at one's own expense as long as the IA communicates reliable RAs.

- The integration of IAs is more better.

National Institute of Informatics

How to connect RA with outside IA

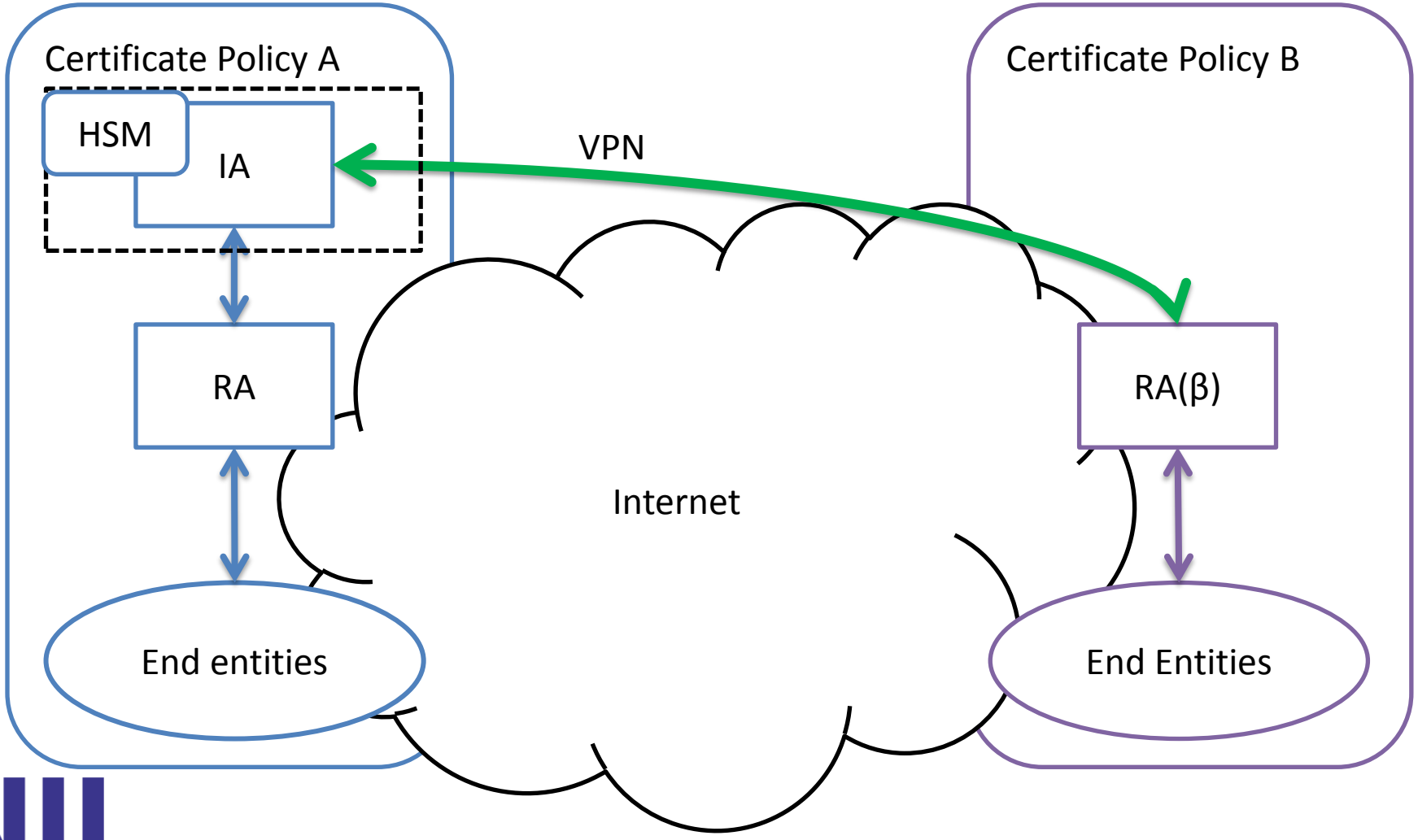


National Institute of Informatics

Proposed IA-RA Connections

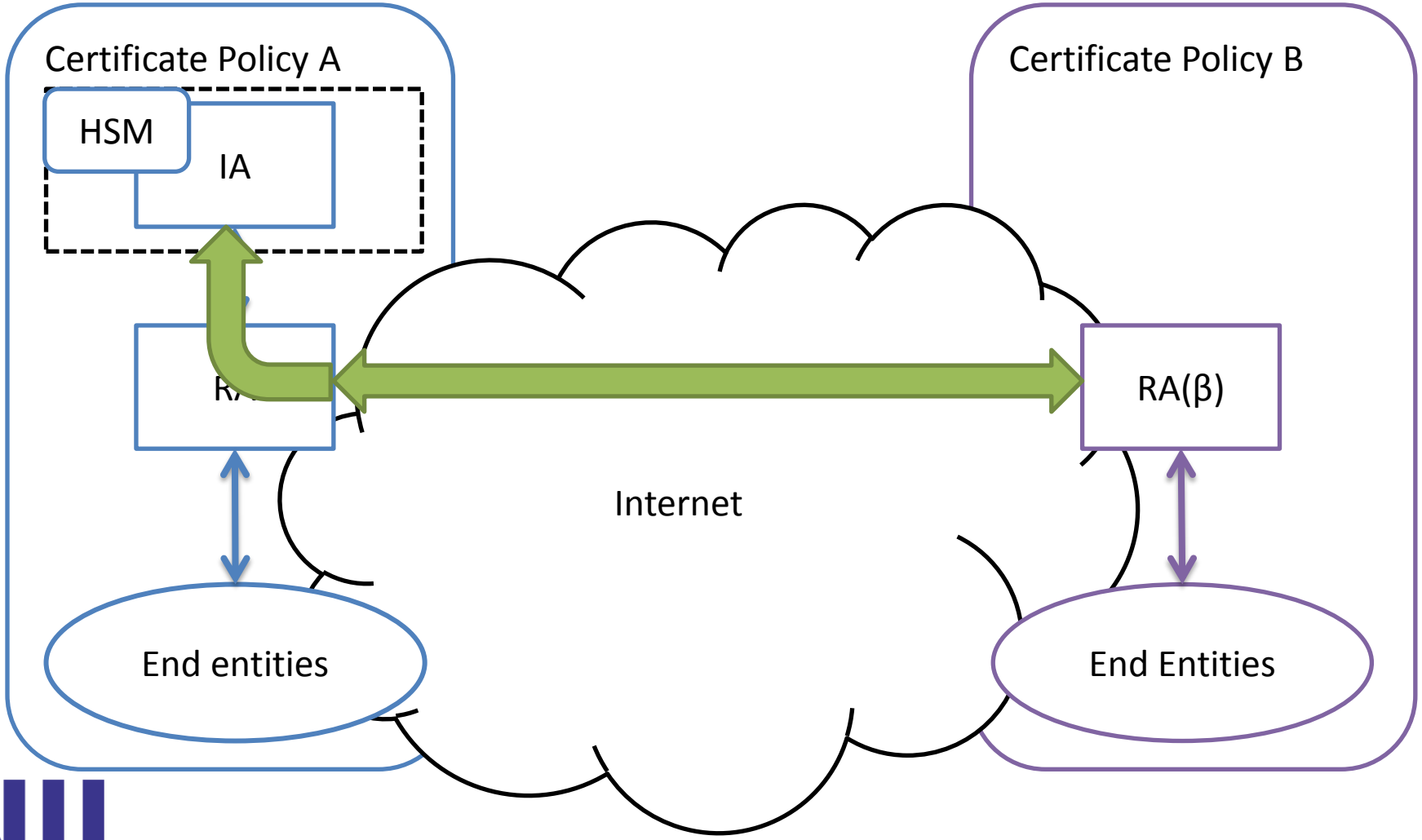
- Direct connection
  - A virtual private network (VPN) connecting between RA(β) and IA.
- Relaying RA
  - Secure connection IA-RA-RA(β) on the public network.

Direct Connecting: VPN



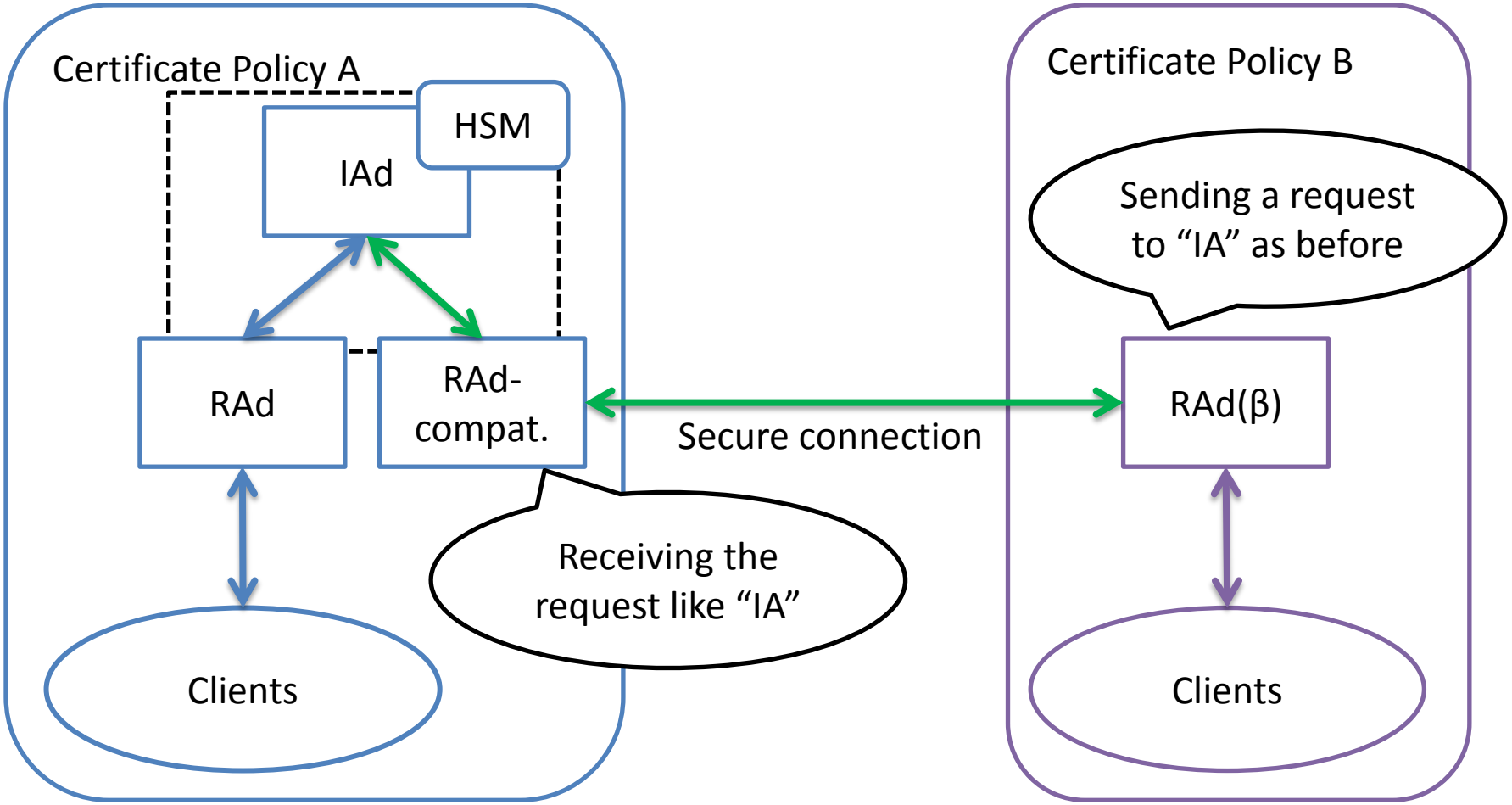
National Institute of Informatics

Relaying RA



National Institute of Informatics

Relaying RA (cont'd)



National Institute of Informatics

Discussion on IA-RA connection

- Direct connecting
  - Advantages
    - Unchanged I/F to users.
    - Basically no software development.
  - Disadvantages
    - Some trouble to establish a VPN.
    - Further difficulty in connecting CA components across countries via VPN
- Relaying RA
  - Advantages
    - Unchanged I/F to users.
    - No difficulty with network infrastructure.
  - Disadvantages
    - Software development is needed.
    - Connection depends on the software package.

National Institute of Informatics

Discussion on AP

- There are two CA authentication profiles that enable CA to issue long-lived certificates, provided by IGTF:
  - Classic
  - MICS (Member Integrated Credential Service)
- An example of 4 combinations
  - IA and RA: MICS, RA(β): Classic
  - RA(β) should change from Classic RA to MICS IdM.
  - This basically ensure each independence of organization and does not interfere in the policy.
  - IA needs to go through the formalities for permit it to issue certificates to the RA(β).

National Institute of Informatics

Related Works

- RPS (Registration Practice Statement)
  - Discussed in IGTF
  - Can be considered as a subordinate document to the CPS
  - It is suggested that separating RAs from the CA function has benefits that are useful for more efficient trust processing of the overall system.
  - RPS framework would help the proposed integration model in policy arrangement.
- ASGC CA as real integrated CA
  - ASGC CA has foreign RAs such as AU, NZ, VN, PH.

National Institute of Informatics

Summary

- We considered an integration model of certificate authorities in a PKI trust federation such IGTF.
- We proposed two connection types between IA and RA:
  - Direct connecting using VPN
  - Relaying RA

- We would like to implement the proposed relaying RA model to NAREGI-CA software and perform demonstrative evaluation.
- We would like to consider integration procedures with RPS framework.

National Institute of Informatics