A Method for Remote Initial Vetting of Identity with PKI Credential

International Symposium on Grids & Clouds 2017
9 March 2017
Academia Sinica, Taipei, Taiwan

Eisaku SAKANE, Takeshi NISHIMURA, Kento AIDA

National Institute of Informatics, Japan

NII
National Institute of Informatics

Outline

- Introduction
- Objects and Issues
- Proposal
- Discussions
- Related Works
- Summary

National Institute of Informatics

Introduction

- Background
  - With the growth of large-scale distributed computing infrastructures, a system that enables researchers to use high performance computing resources in such infrastructures has been established.
  - It is tough to carry out *initial* vetting of identity based on a face-to-face meeting at a window for the system if the researcher whose proposal is accepted lives in a foreign country.
    - Anyone can apply a research project proposal to HPCI in Japan.
    - HPCI needs to vet the identity of foreign user based on a face-to-face meeting if their proposal is accepted.

National Institute of Informatics

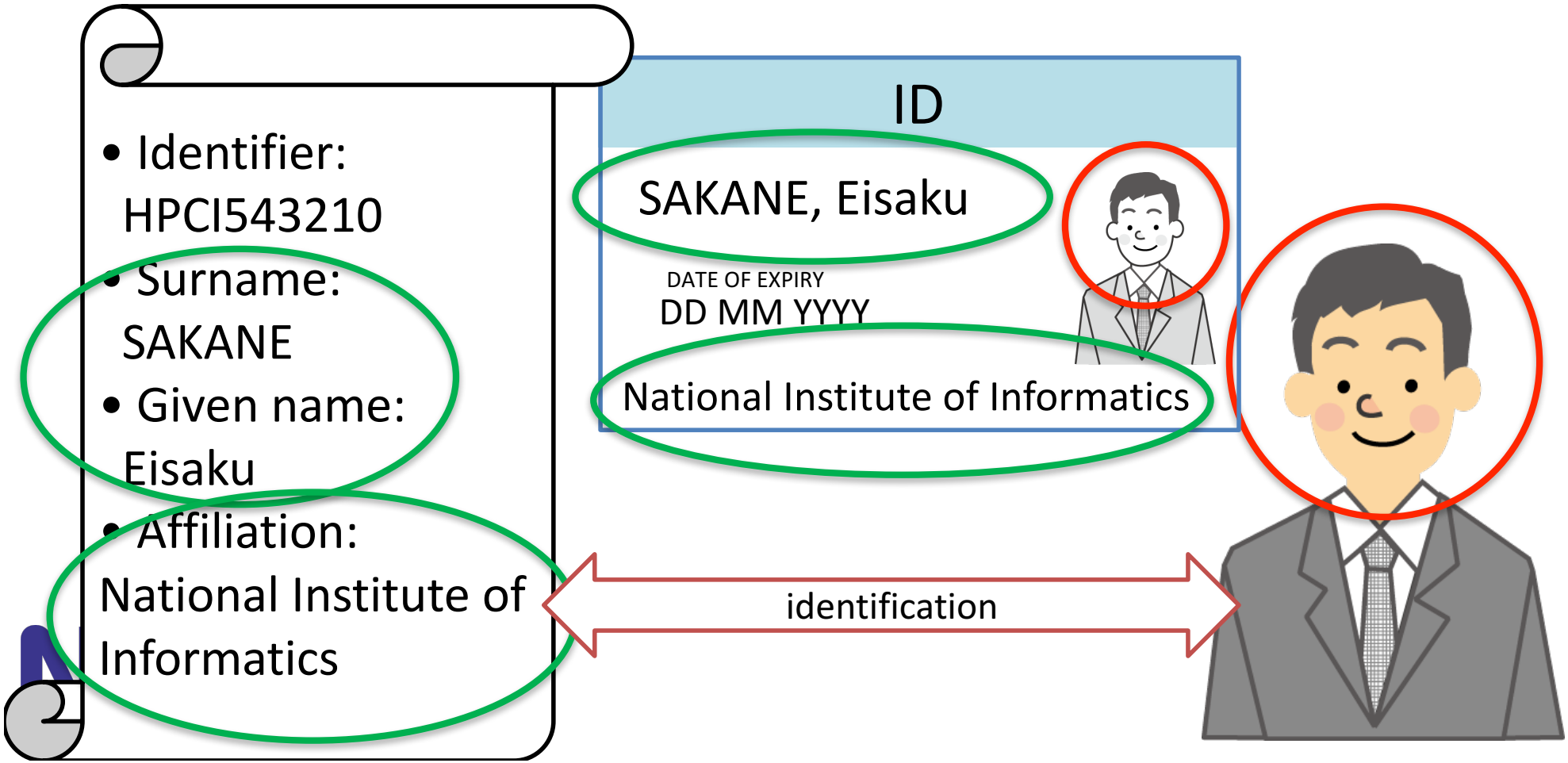
Introduction (cont'd)

- Guiding question
  - How does the system vet the identity of user who cannot come to a window for the system ?
  - It is an important issue to establish a remote initial identification procedure.
- Importance of the research
  - We propose a method for remote initial vetting of identity with PKI credential.

National Institute of Informatics

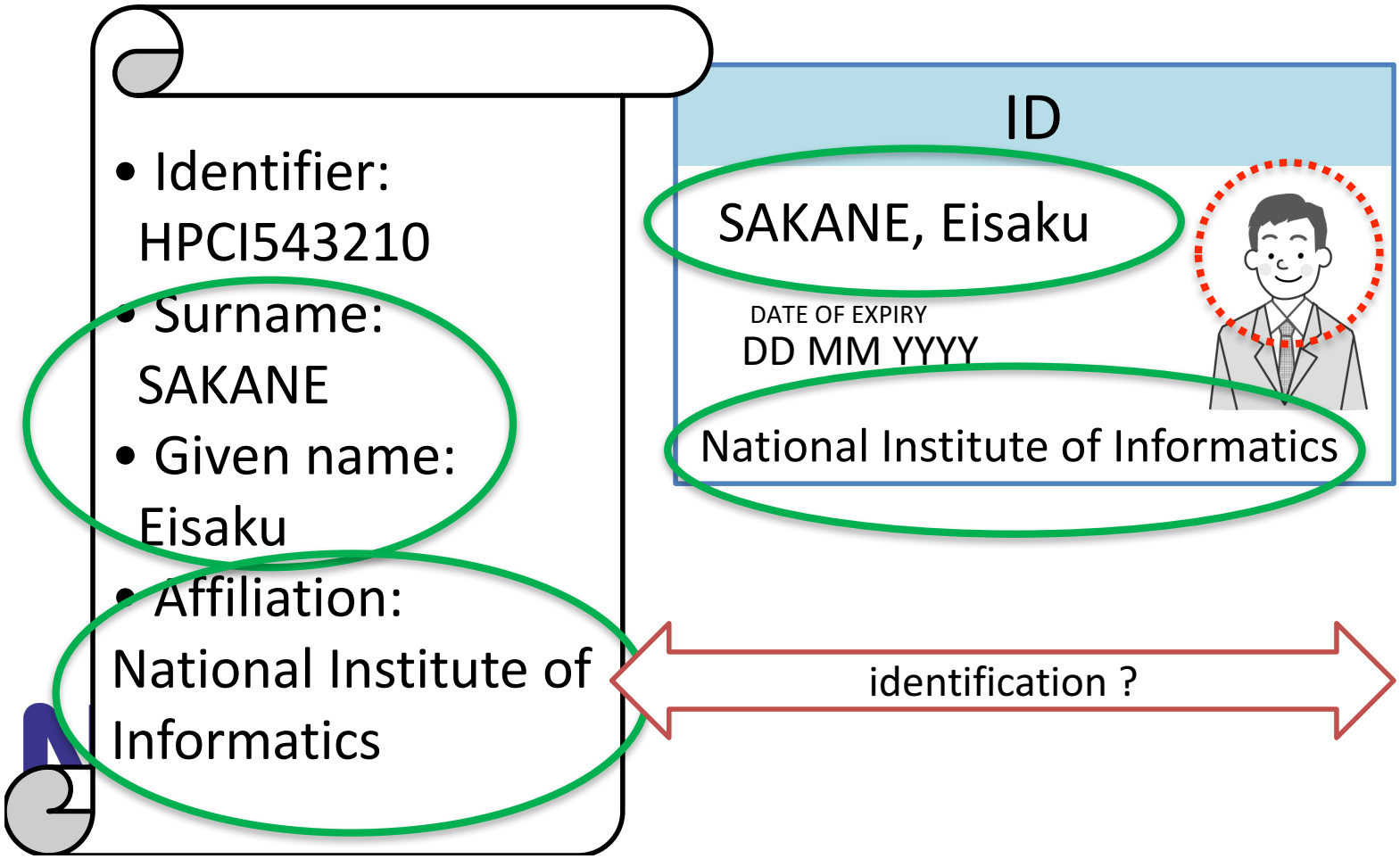
Initial F2F Identity Vetting

- The aim of identity vetting is to check identity data against photo-ID and/or valid official documents.



Initial F2F Identity Vetting

- The aim of identity vetting is to check identity data against photo-ID and/or valid official documents.



Basic Idea

- A trust federation is composed of IdPs and SPs.
  - Each IdP in the trust federation ensures the same level of identity vetting.

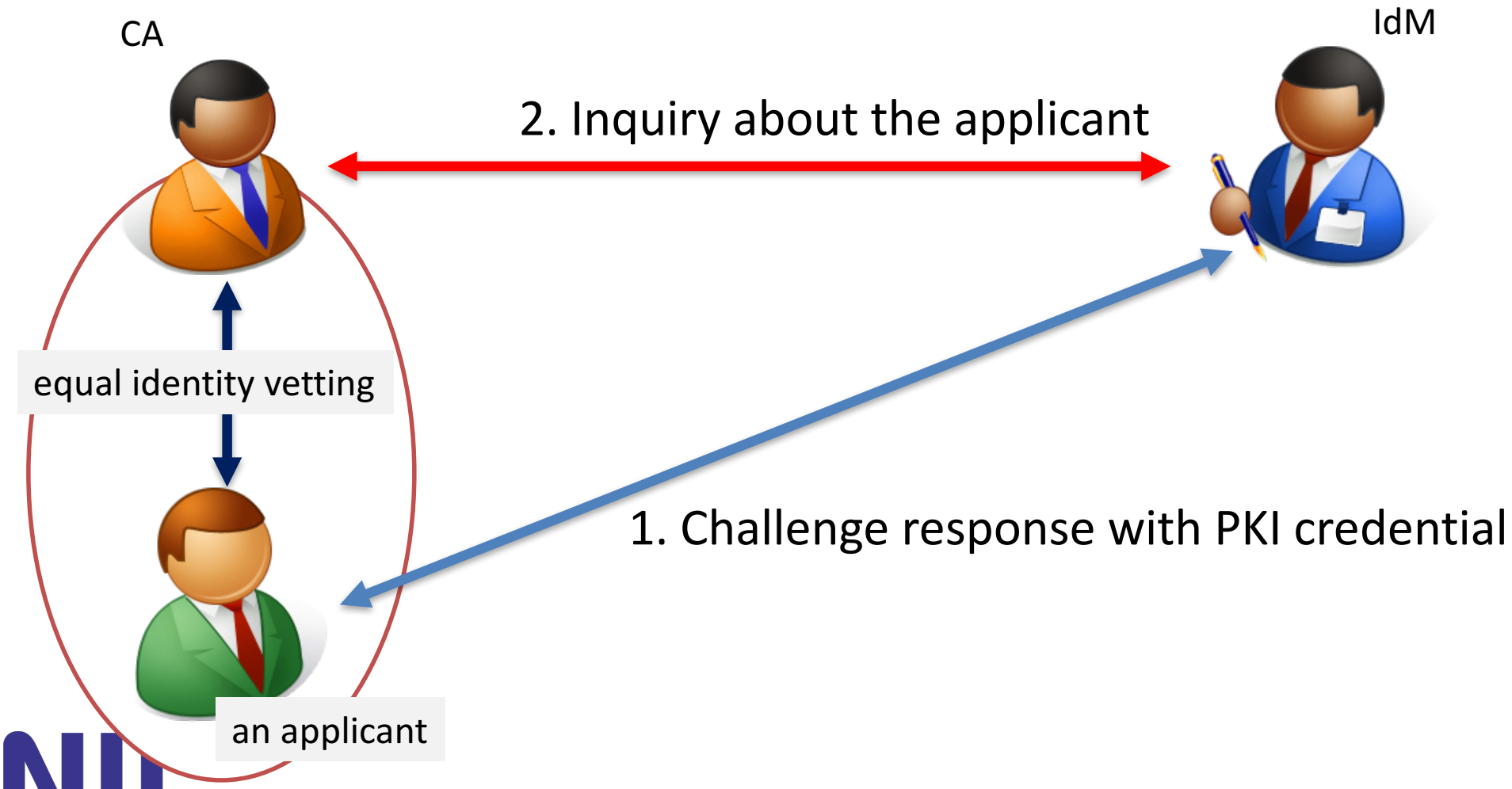
- Abandoning an attempt for the system itself to vet the identity of an applicant.
- Instead, using a credential generated by the identity data already confirmed based on a equal identity vetting.

NII
National Institute of Informatics

Basic Idea (cont'd)

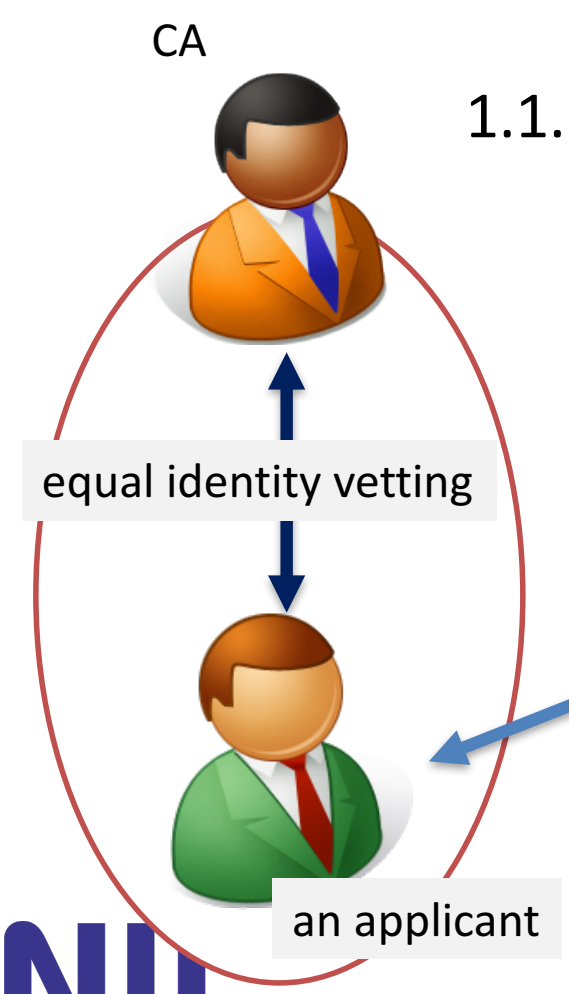
National Institute of Informatics

Proposed Process with PKI Credential



National Institute of Informatics

Challenge Response with PKI Credential



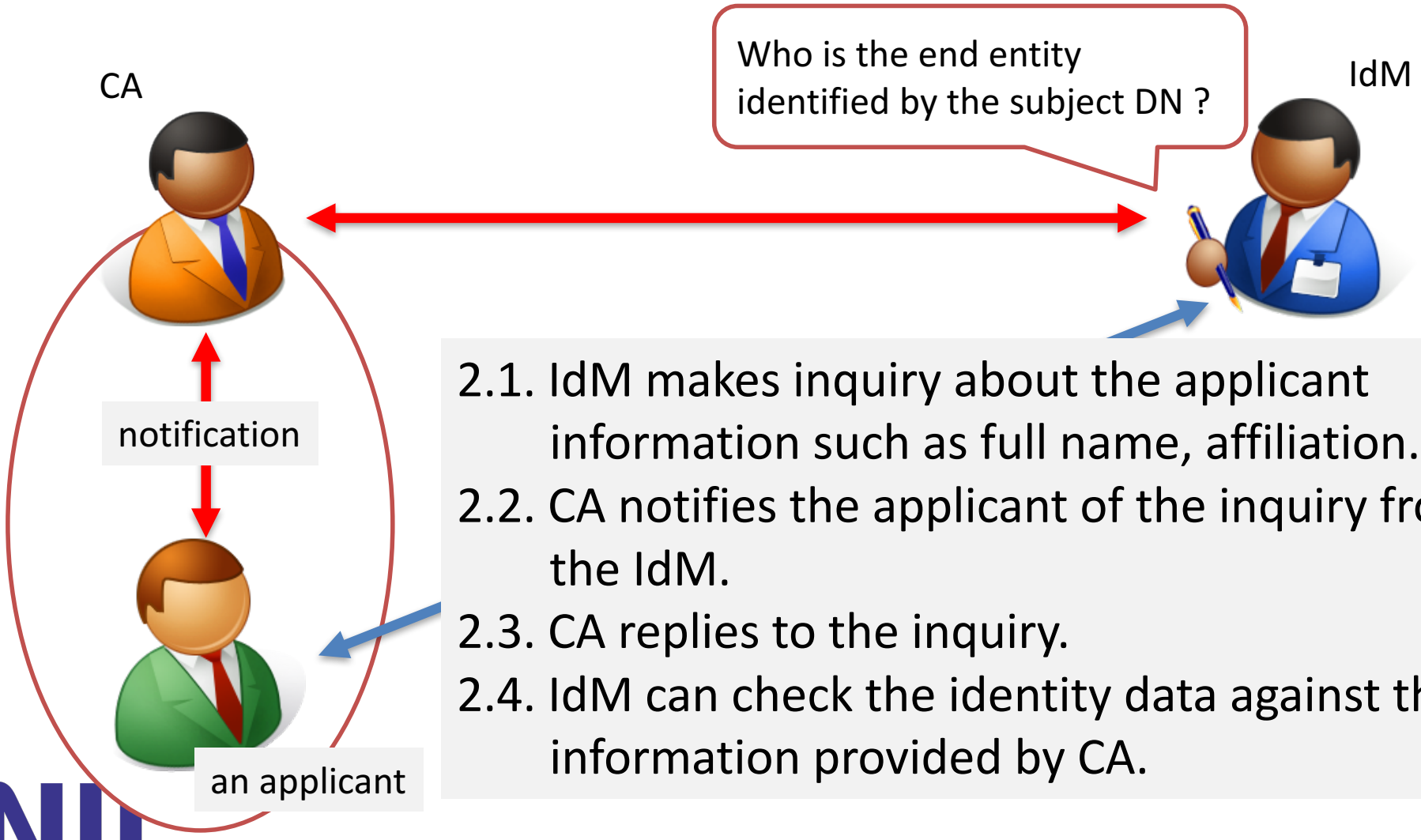
1.1. IdM relies on CA that ensures the same level of identity assurance. Also CA consents to reply to an inquiry from IdM.

1.2. IdM does a challenge response to an applicant.

1.3. IdM obtains the subject DN of the applicant.

National Institute of Informatics

Inquiry about the Applicant



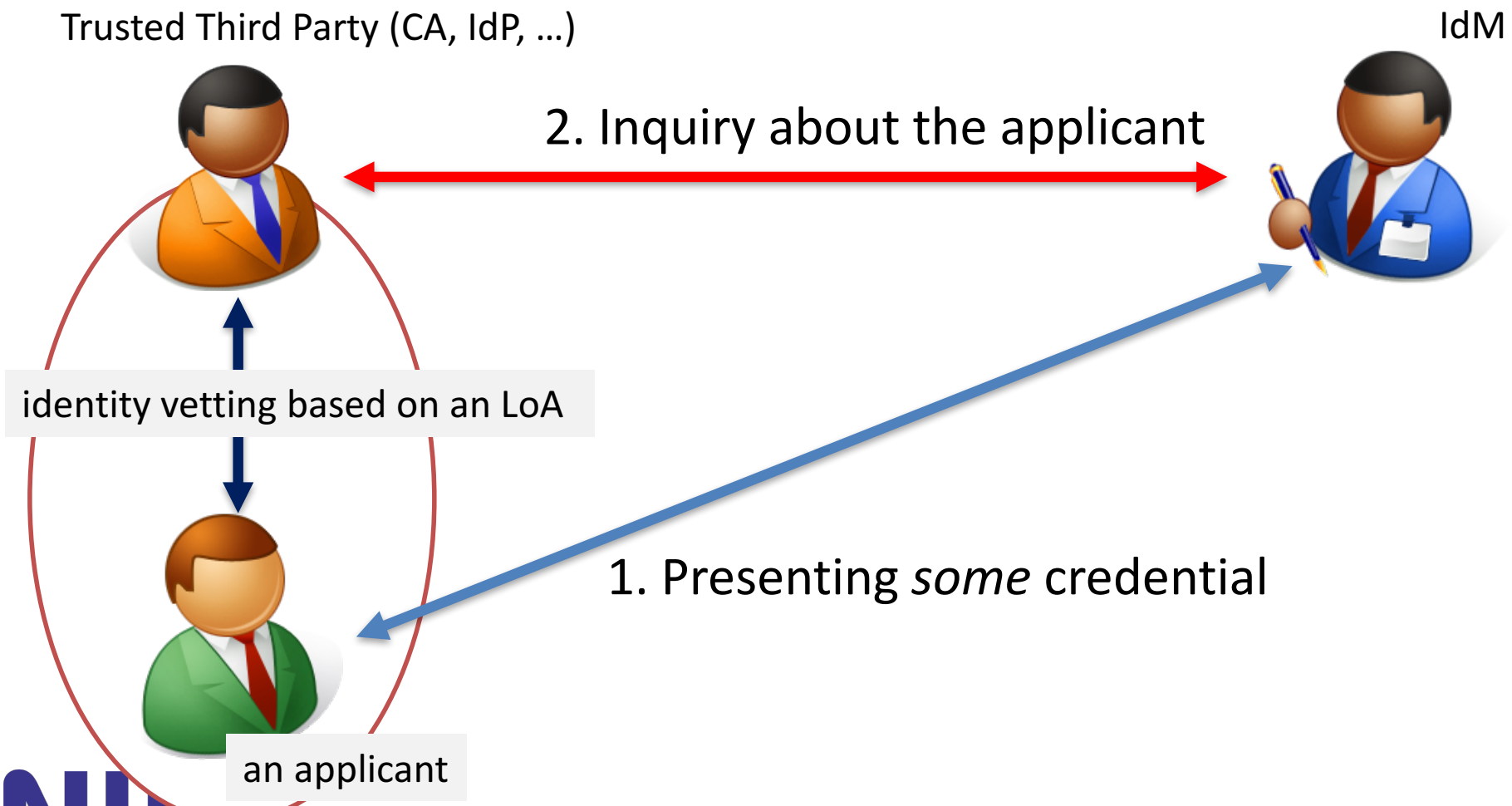
2.1. IdM makes inquiry about the applicant information such as full name, affiliation.
2.2. CA notifies the applicant of the inquiry from the IdM.
2.3. CA replies to the inquiry.
2.4. IdM can check the identity data against the information provided by CA.

National Institute of Informatics

Discussion

- Why is the inquiry about the applicant needed ?
  - Necessary information cannot always be read from the subject DN.
  - Even if necessary information used in checking can be read from the subject DN, CA should notify the inquiry from the IdM and confirm that the inquiry is valid in the identity vetting by the IdM because the applicant is not in the presence of the personnel of the IdM.
- Can existing credentials be used for authentication in accessing services such as HPC resources ?
  - The proposed method is for *initial* vetting of identity.
  - Whether the credential used in the initial vetting of identity can be used for authentication in services is different problem.

Generalization



National Institute of Informatics

Related Works

- Video-supported identity vetting guidelines
  - http://wiki.eugridpma.org/Main/VettingModelGuidelines
  - implement a remote identity vetting process with a video conference between an applicant and a verifier.
- Policy harmonisation by AARC
  - https://aarc-project.eu/workpackages/policy-harmonisation/

National Institute of Informatics

Video-supported Identity Vetting

National Institute of Informatics

Summary

- We considered a method for remote initial vetting of identity.
- We proposed a process for remote initial vetting of identity with a PKI credential among an applicant, an IdM, and a CA that issued the certificate to the applicant:
  - Challenge response between the applicant and the IdM with the PKI credential
  - Process between the IdM and the CA
- We will evaluate the proposed method and discuss application to the identity vetting process in HPCI.

National Institute of Informatics