Consolidated Privilege Management and Authorization for Loosely-Hierarchical Organizations: the Practices in Chinese Academy of Sciences

Jingqiang Lin

Institute of Information Engineering,

Chinese Academy of Sciences

CANS 2017, Kunshan, CHINA

Outline

- Consolidated Identity & Access Management System in Chinese Academy of Sciences
- Privilege and Authorization of Loosely-Hierarchical Organizations: Requirements
- Consolidated Privilege Management and Authorization
  - Design
  - Progress

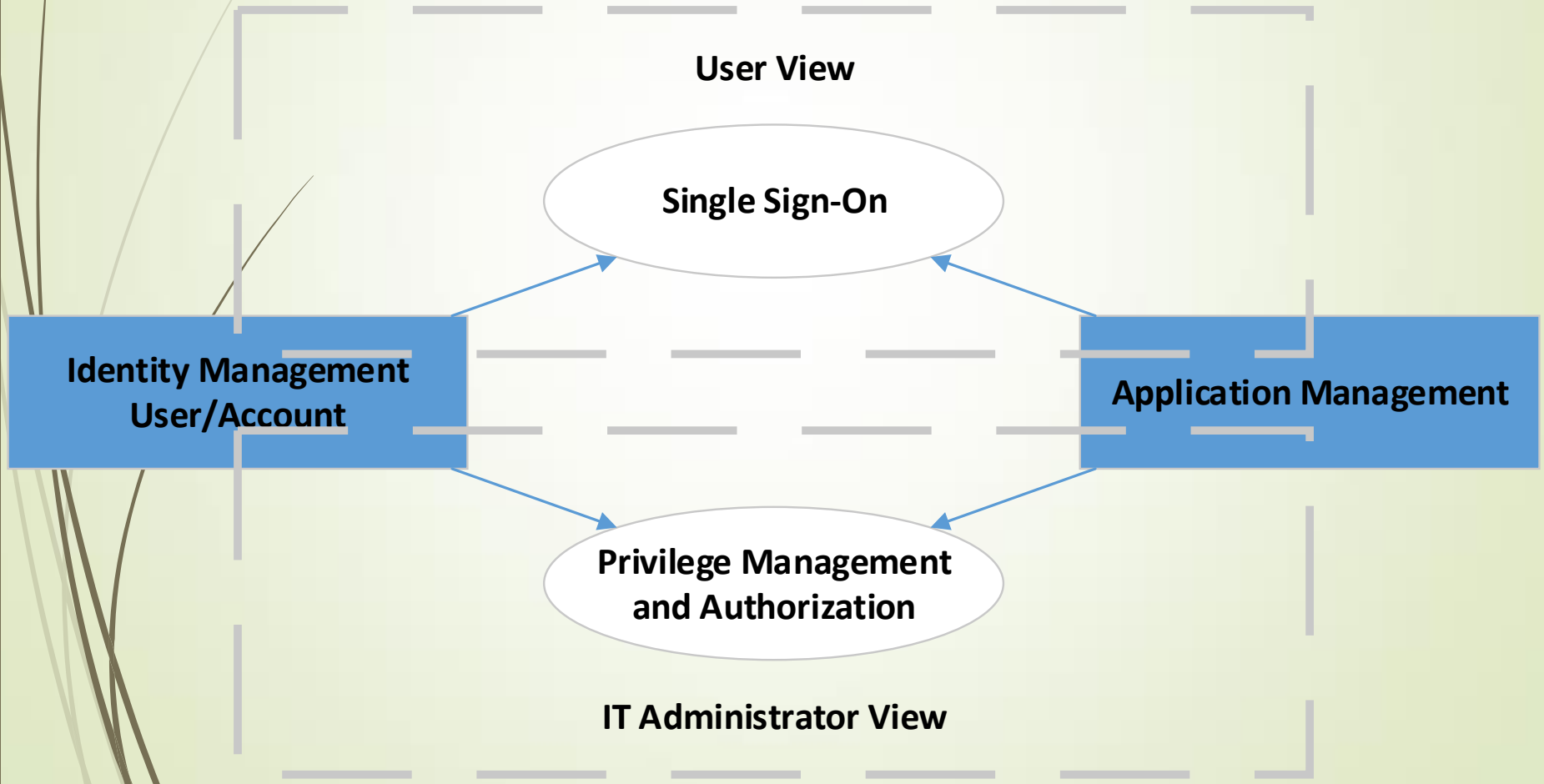
Consolidated Identity & Access Management System

- Designed and built for Chinese Academy of Sciences (CAS)
  - Since 2011, in progress
  - Being used, and also being improved
- Our goal (dream): Identity & Access Management
  - 100+ institute of CAS
  - 60k+ employee, 52k+ student
  - Cross-institute/university applications
    - Hundreds of? Thousands of? Hundreds of thousands?

The CIAM-CAS system

Functionality of CIAM

- Consolidated Identity & Access Management

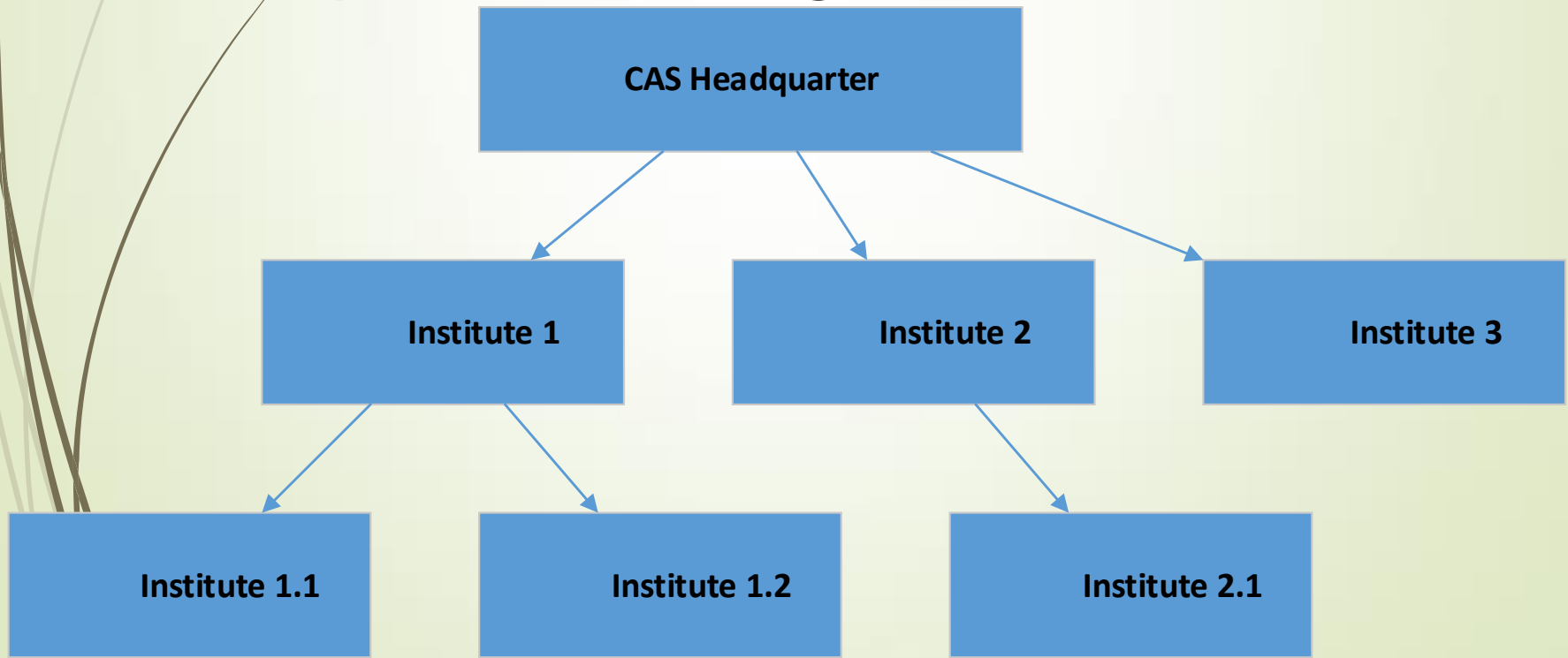


Functionality of CIAM

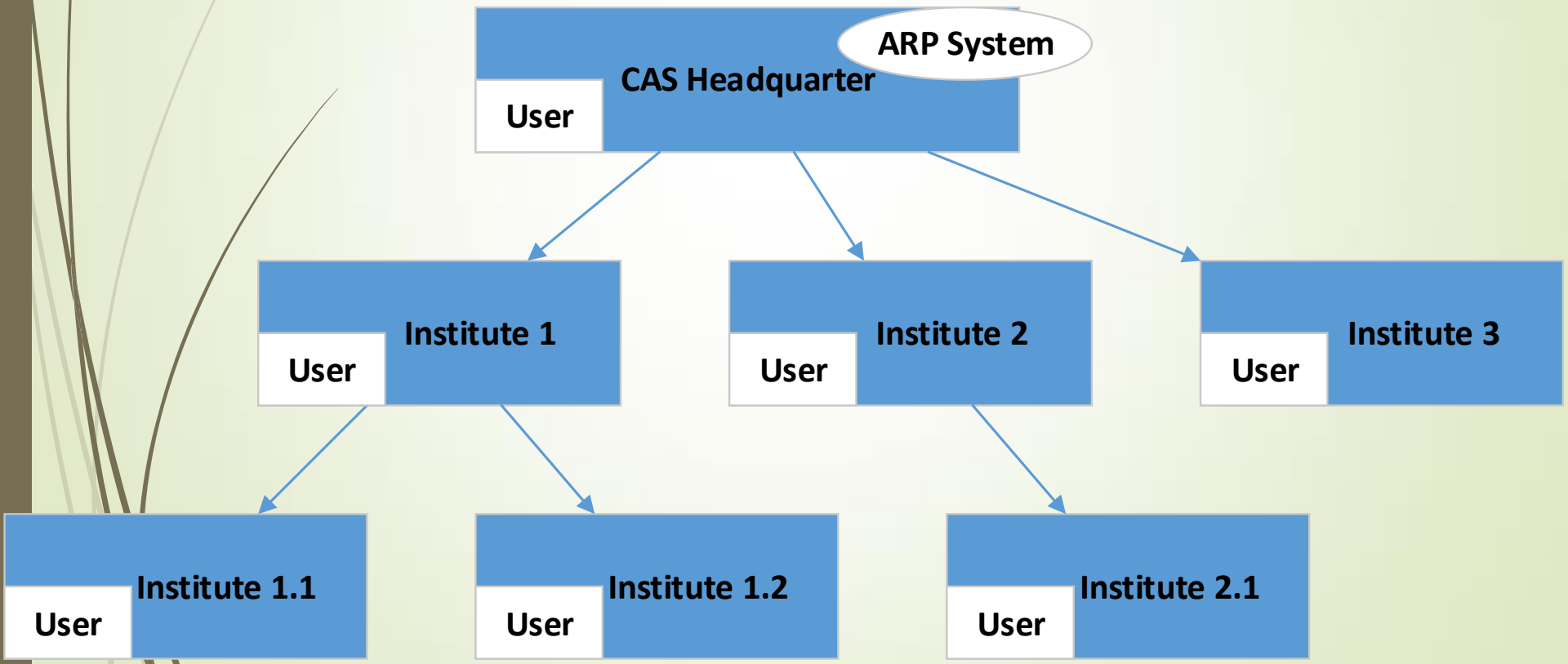
- Single Sign-On Standard
  - OpenID, OAuth, SAML, OpenID
  - …
- Privilege Management and Authorization
  - It depends on the structure of consolidated organizations
    - Hierarchical organizations
    - Independent institutes
    - …

The structure of CAS

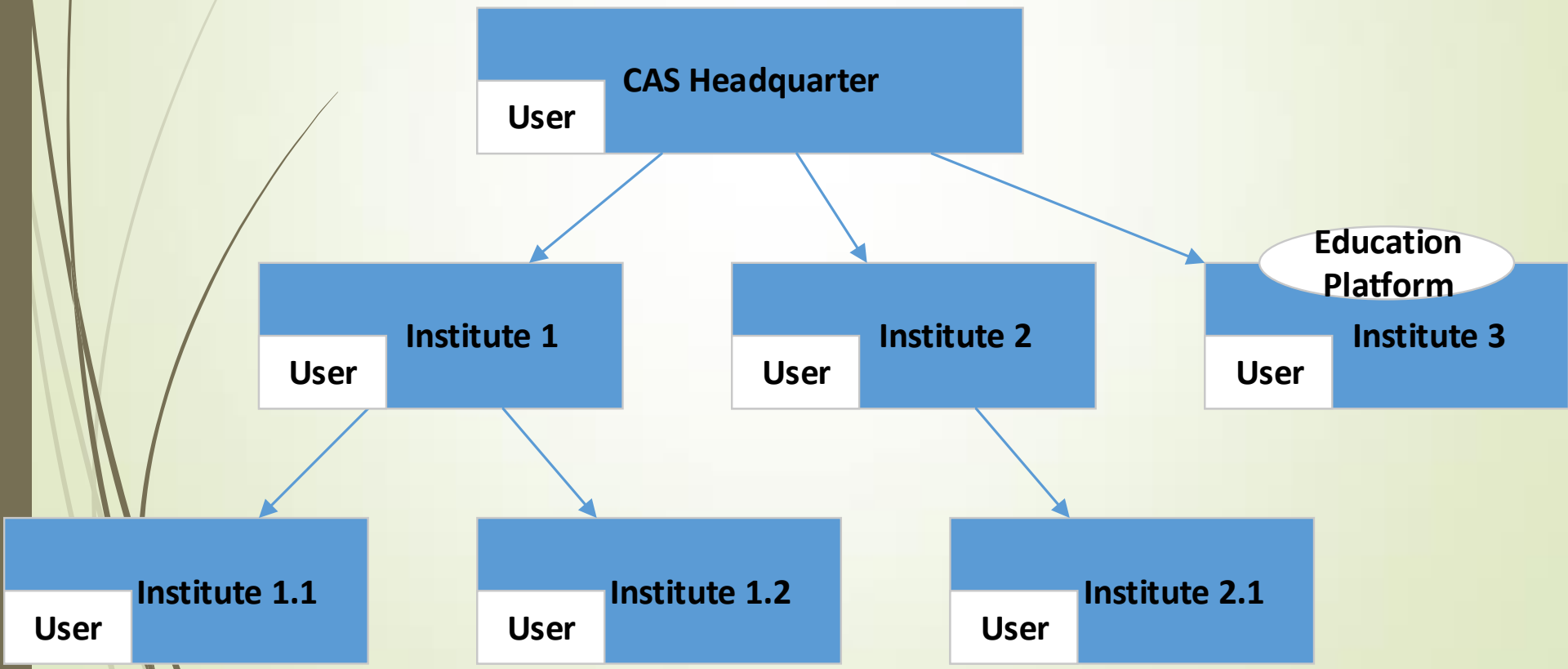
- Chinese Academy of Sciences
  - Headquarter
  - Subordinate institutes
- Loosely-Hierarchical Organizations



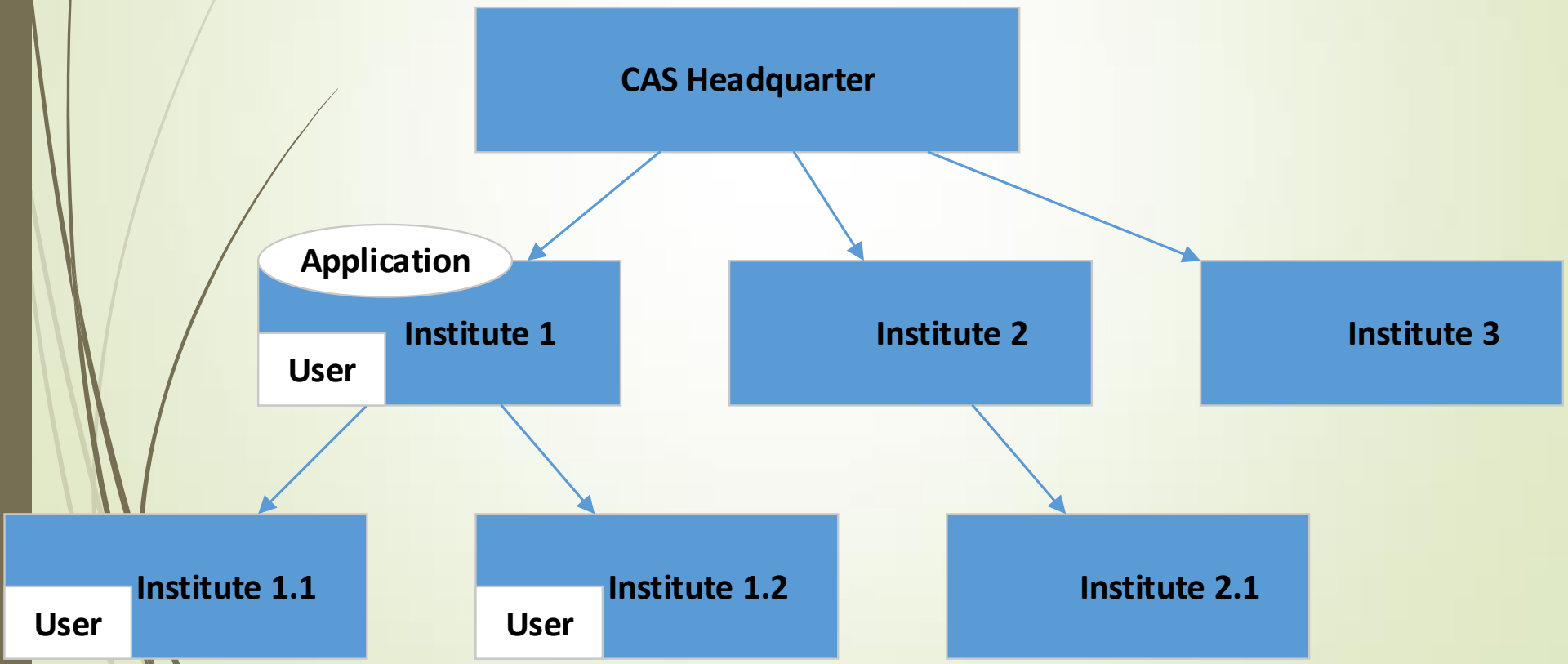
Cross-institute Application (Example)



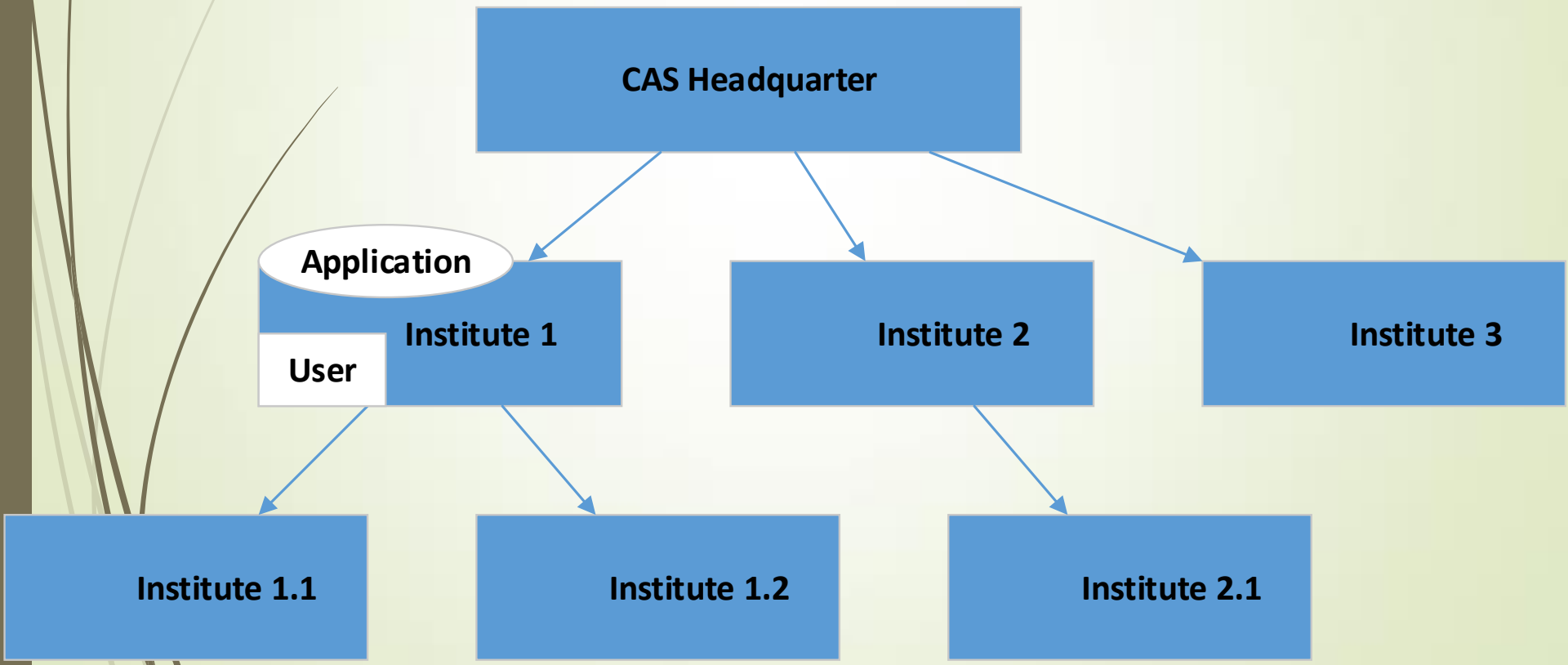
Cross-institute Application (Example)



In-institute Application (Example)



In-institute Application (Example)



Consolidated Privilege Management and Authorization

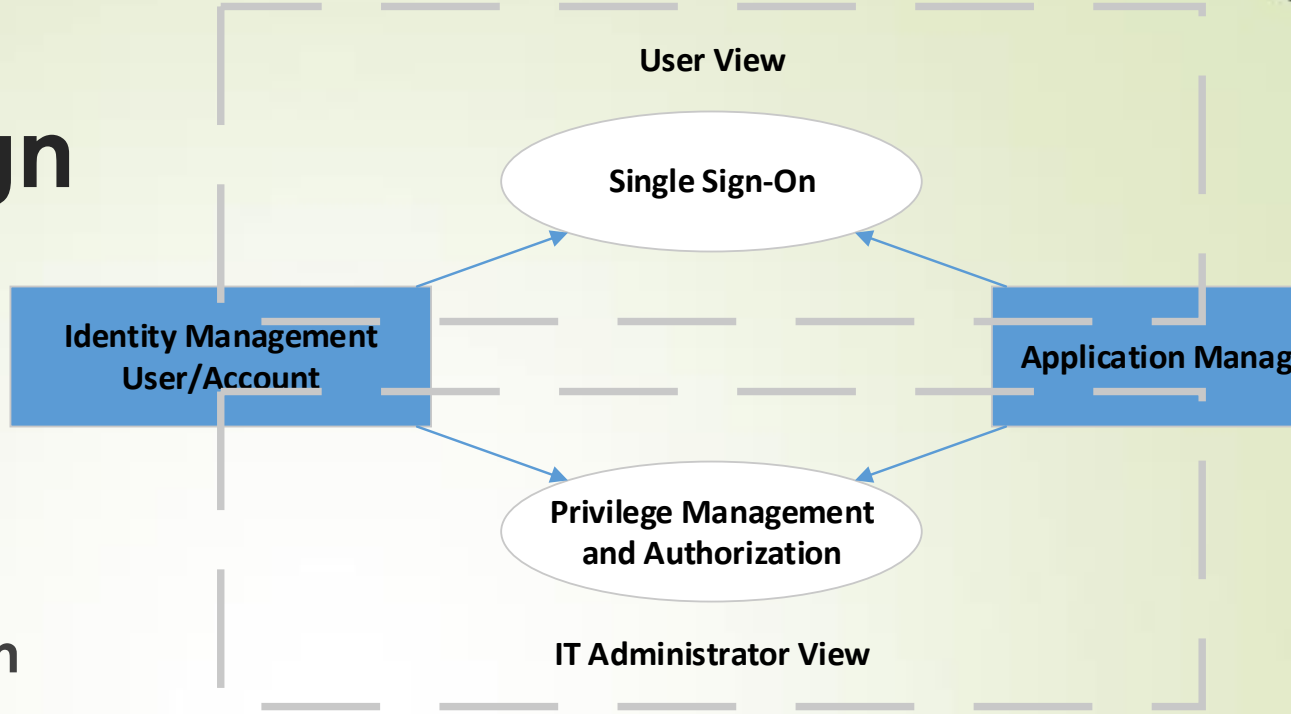
- Privilege Management and Authorization
  - Work cooperatively with Identity Management & SSO

- Goals
  - Security, least privilege
  - Flexibility, for diverse requirements
  - Autonomy, final control by the owner institute
  - Convenience, easy to configure

Consolidated Privilege Management and Authorization

- Privilege Management and Authorization
  - Not designed for the privilege and authorization within an application
- Our scope, to answer two questions
  - Who can access a cross-institute application?
  - Who can manage it?

Our Design



- Role
  - Manager
  - User
  - Application
- Privilege and Authorization
  - Manager -> User/Application
  - User -> Application
- Principle
  - Hierarchical rules + loose rules

Role

- Strictly-hierarchical structure
  - Institutes are organized hierarchically
- Each institute has its own managers
- Each application belongs to one institute
  - Only one
- Each user belongs to one institute
  - At least one, maybe multiple occasionally
  - Flexibility

Privilege and Authorization - Manager

- <Manager M, Institute I>
  - M manages I and all institutes subordinate to I – Default hierarchy
    - M is considered as a manager of institutes subordinate to I
  - Privileges of M, are degraded as the levels change – Loose hierarchy
    - Mandatory privilege: enforced in all subordinate institutes
    - Restricted privilege: only in limited levels
    - Private privilege: only in I

Typical Privileges of Managers

- Privileges
  - Add/Delete users
  - Add/Delete application
  - View/query
- Can be enforced as
  - Mandatory privilege: enforced in all subordinate institutes
  - Restricted privilege: only in limited levels
  - Private privilege: only in I
- Answer the question
  - Who can mange the access of user to application?

Privilege and Authorization - User

- <User U, Institute I>
  - U is a user of I, also a user of any supreme institute – Default hierarchy
    - U is able to access all these applications
    - More special role/attribute-based access controls will be enforced WITHIN applications

Privilege and Authorization - User

- <User U, Institute I>
  - Privileges of U, are degraded as the applications change – Loose hierarchy
    - Protected application of Institute I
      - Accessible to all users of I and all subordinate institutes
    - Public application
      - Accessible to all users of I and all subordinate institutes
      - Granted to the users other institutes, by its managers
    - Private application
      - Accessible to only the users of I
- Answer the question
  - Who can access a cross-institute application?

Feature

- Security, least privilege
  - Private privilege
  - Private application
- Flexibility, for diverse requirements
  - Privilege: Mandatory > Restricted > Private
  - Application: Public > Protected > Private
- Autonomy, final control by the owner institute
  - Each institute has its own managers
  - With private privileges and private application
- Convenience, easy to configure
  - Only a little number of configuration rules are enough

Work-in-Progress

- Consolidated Identity & Access Management System in Chinese Academy of Sciences
  - The development started in about 2011
  - It is being used and being improved
    - SSO works well
- Privilege Management and Authorization
  - Not so good/friendly for IT managers
  - We are working on it, since 2016 …

Thanks!
Any comments are welcome!

Jingqiang Lin linjingqiang@iie.ac.cn

Institute of Information Engineering, Chinese Academy of Sciences