Realization of a Lightweight Account Management System Supporting Campus Members with Various Status

Hirokatsu SEGAWA, Takahiko Tsujisawa and Miyuki Ishibashi

Information Media Center
Tokyo University of Agriculture and Technology
Tokyo, Japan

Agenda

1. In General
   - User account, Authentication and Authorization
   - User account management process
2. In (Japanese) Universities
   - Peculiar circumstance and problems
   - Our idea and system design
   - Our account management system

User account

- Allowing a user to authenticate to system service
- Being granted authorization to access system service
- Typically method:
  Using a combination of a user ID and their secret password

Authentication and Authorization

- Authentication
  - Checking a proof of identity
  - Checking the requisite attributes
- Authorization
  - Specifying access rights to resources
  - Typically method:
    Using the defined access control rules
    (an access control list / capability)

User account management process

- For various information services,
  - Issuing a new account
  - Changing its authorities (as necessary)
  - Changing its attributes (as necessary)
  - Disabling or deleting the account

    ...

Who can get the account ?

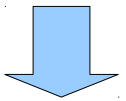
- In universities:
  - Students
    - Regular students, short-term exchange students, ...
  - Faculties and Staff
    - Regular employment, Irregular (ex. part-time) employment, ...
  - Others
    - Visiting researchers, secretaries who are paid by private funds, ...

Members in our university (TUAT)

- Students: 6000
- Faculties and staff: 1700
  - Regular employment: 700
  - Irregular employment: 1000
- Others: ? (not accurately grasped)

Our circumstances

- No explicit definition for campus members
  - Various status members are managed by each section by their own policy
- No explicit policy for account management
  - Various information services are managed by each section by their own policy

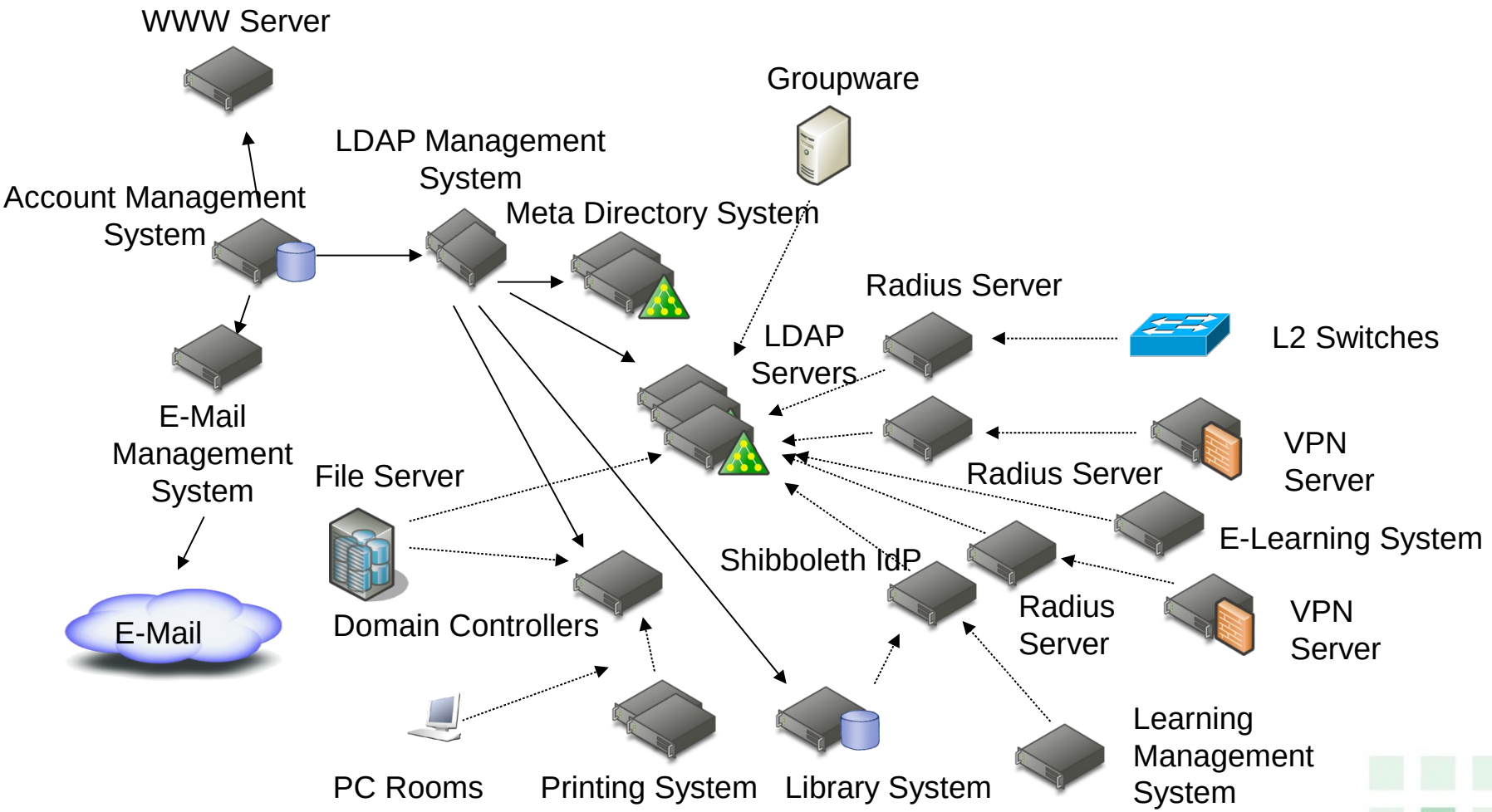


- Short-term exchange students; yes or no ?
- Part-time employment staffs; yes or no ?

Problems in our circumstance

- Constructing trusted databases for human resources is not easily.
- Different operation policies often make some exceptions (irregular operations by manually).
- Getting data for authentication and authorization is not easily.

Our main services



Example of member's status

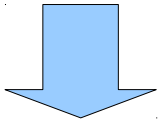
Status	Staff A	Staff B	Staff C
Management Section	Section *a*	Section *b*	Section *a*
Available Services	Educational affairs, E-mail, Financial affairs, Network, PC room, Groupware, Shared storage	E-mail, Financial affairs, Network, Shared storage	E-mail, Network

If a user makes an application for his or her account, ...

- Checking which section manages an applicant
- Checking whether an applicant can use the service or not
- Checking attributes (personal data) that service requires and getting them from each section
- Converting raw data to adapt to the system
- Registering converted data to the system and creating applicant's account
- Issuing user ID and password to an applicant

Ideal system

- Explicit definition for campus members
- Unique trusted database
- Unified policy for issuing an account
- Unified authentication and authorization scheme

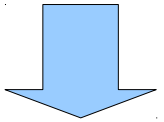


Users could access each service by their own single account

Ideal system

- Explicit definition for campus members
- Unique trusted database
- Unified policy for issuing an account
- Unified authentication and authorization scheme

Could not



Users could access each service by their own single account

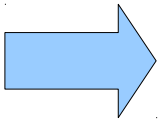
Why we could not ?

- It is too difficult to unify:
  - Databases storing personal data in each section
  - Management policies for services or systems in each section
  - Operation policies for services or systems in each sections

We do not have enough resources ...

Our idea

- A lightweight system;
  - Be adaptable to campus members with various status.
  - Be adaptable to databases storing personal data managed by different polices.
  - Be adaptable to services or systems managed by different policies.



Mediating between the different policies

System design

- Web-based user interface
  - For users and operators
- Compact database
  - No replications of original data
- Simple data format for the registration
  - For various services

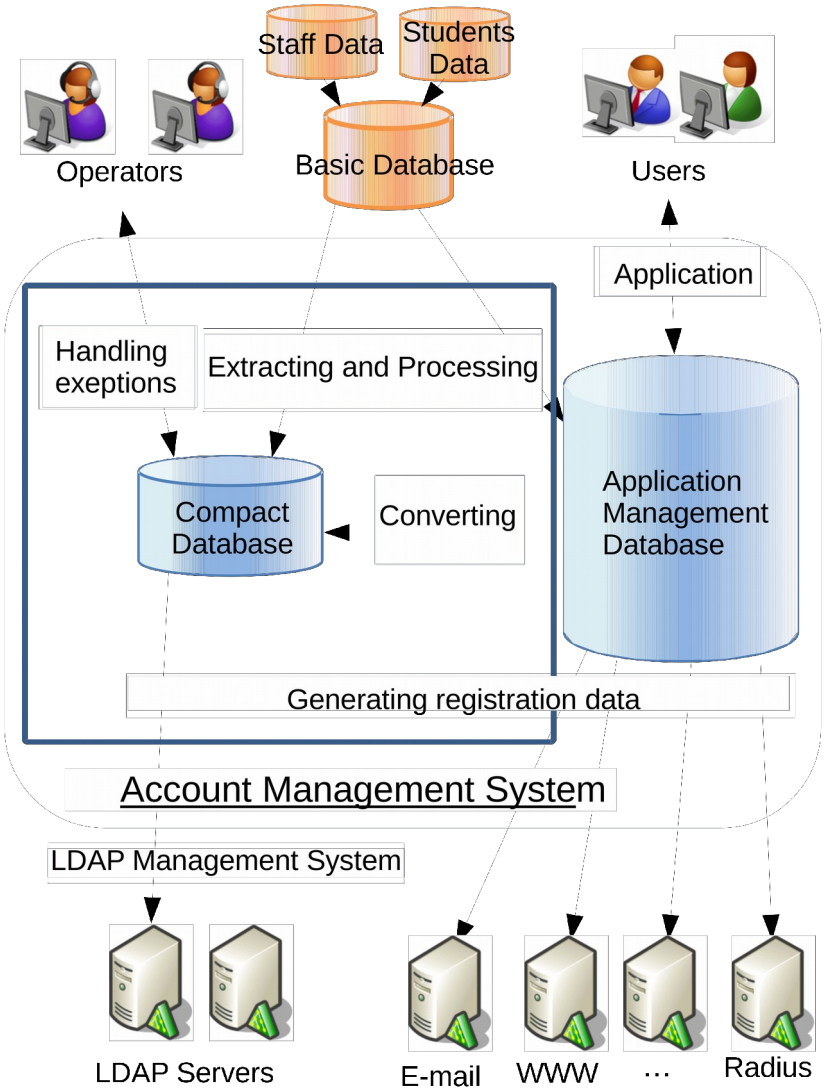
Basic functions

- Accepting user's requests
  - Issuing a new account
  - Changing user's password
  - Disabling user's account
- Assigning (or removing) an account to a service
- Registering (or excluding) user's ID and password to authentication systems

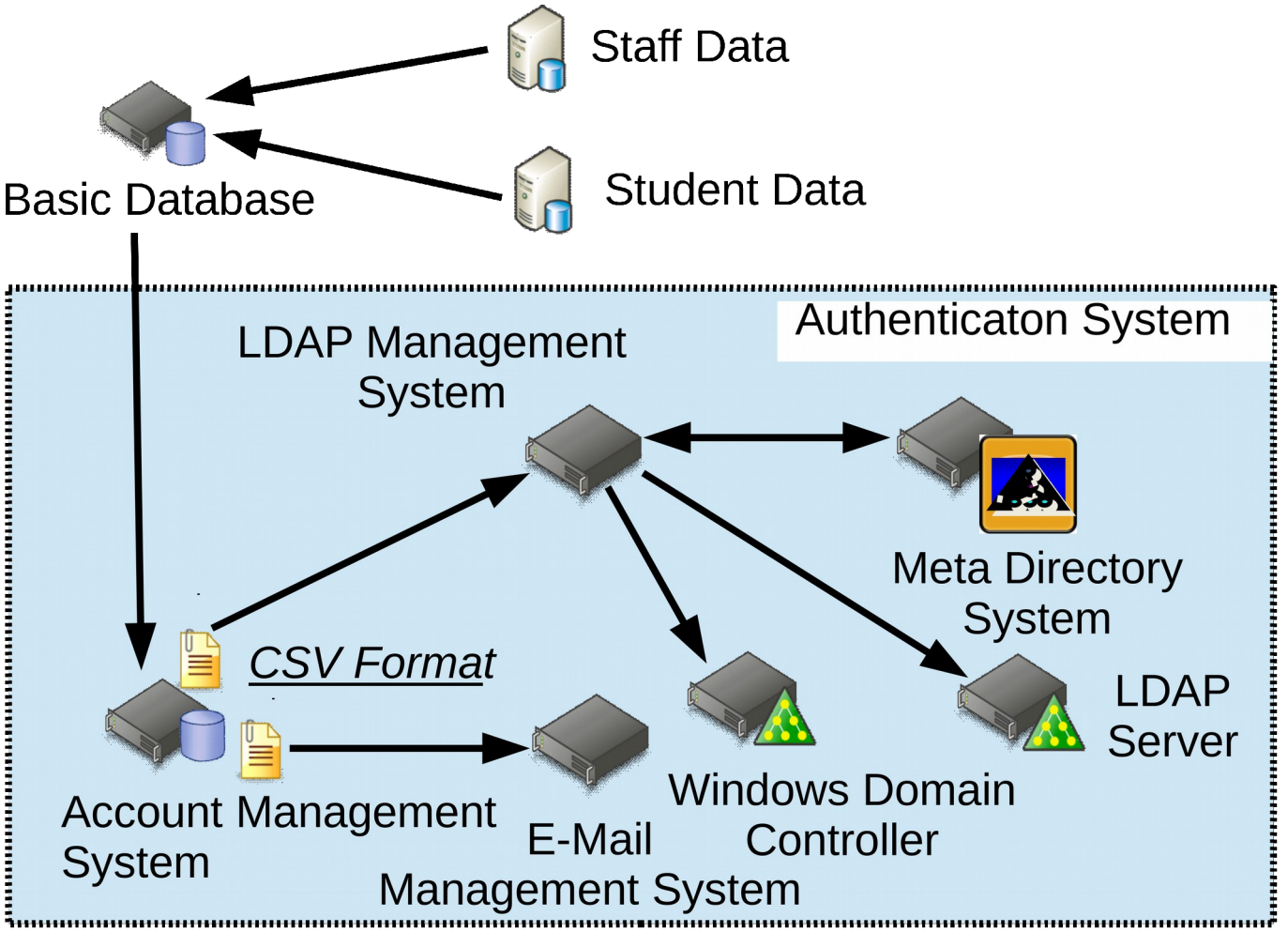
Features

- Gathering raw data for accounts from each management section
- Processing raw data, in order to adapt requirements of the system automatically by predefined rules
- Sending registration data in the form of a simple CSV file to each system
- Being able to handle exceptions
  - For invalid data, special treatments, ...

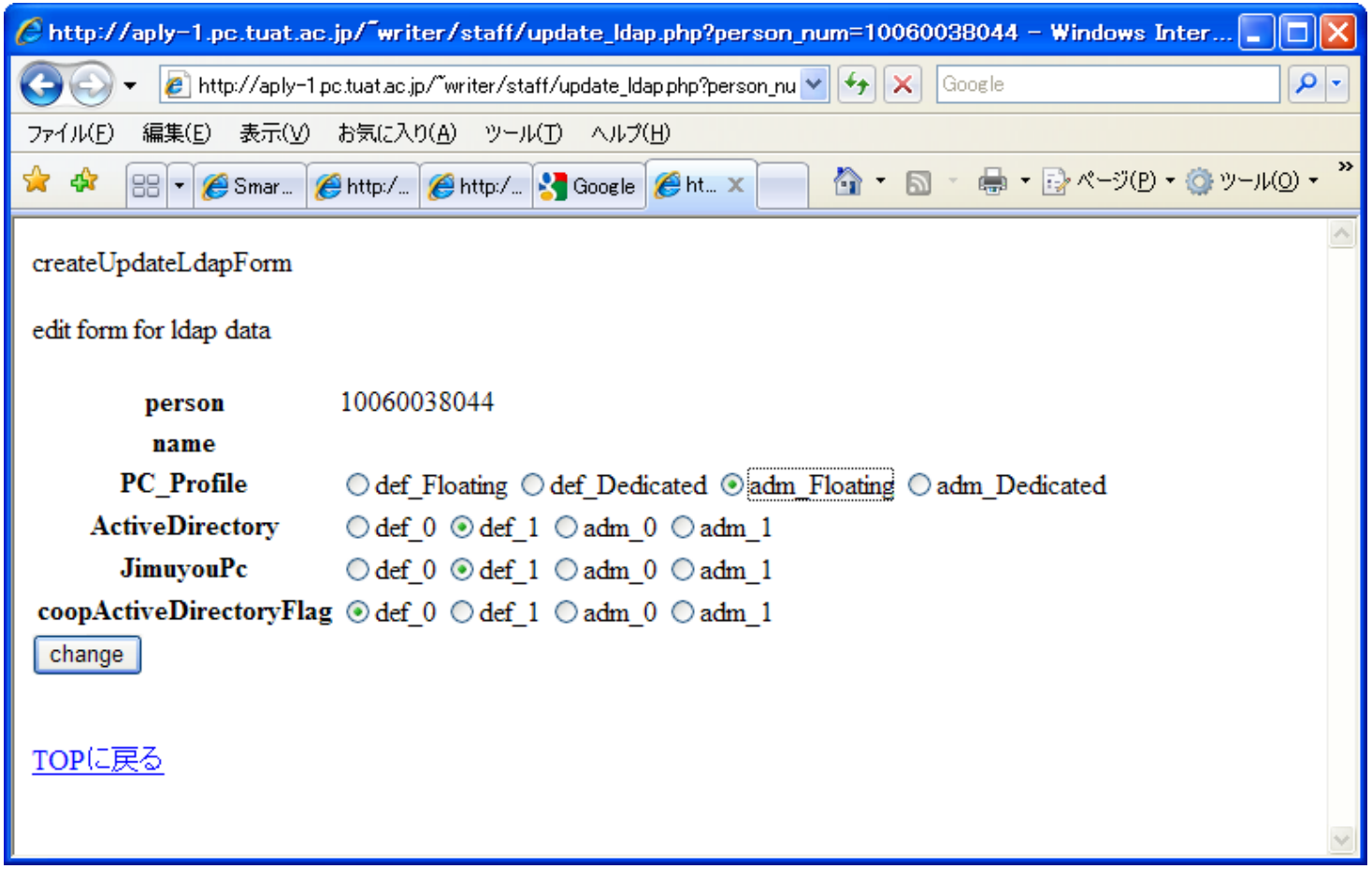
Our account management system



Process of issuing an account



Web-based user interface



Furthermore

- Improving the system robustness (such as system redundancy)
- Improving the unification of authentication
- Improving the adaptability to “GakuNin” (Academic access management federation in Japan)
- Coping with Single Sign-On

Conclusion

- We have developed a lightweight account management system.
  - This can support various kinds of services and systems.
  - It is possible to cooperate with a new system which will be provided in near future.
  - We did not reconstructing databases storing personal data.