

# Identity Management - ORION implementation

**EurOpen.CZ**  
**XXXth conference**

**Jiří Bořík, University of West Bohemia**

# Contents

- The ORION computing environment
- Data sources consolidation and CRO project
- Current ORION Identity management activities – Sun Java System Identity Manager and Grouper
- Provisioning strategy
- Roles and workflows
- Conclusions

# ORION Computing Environment

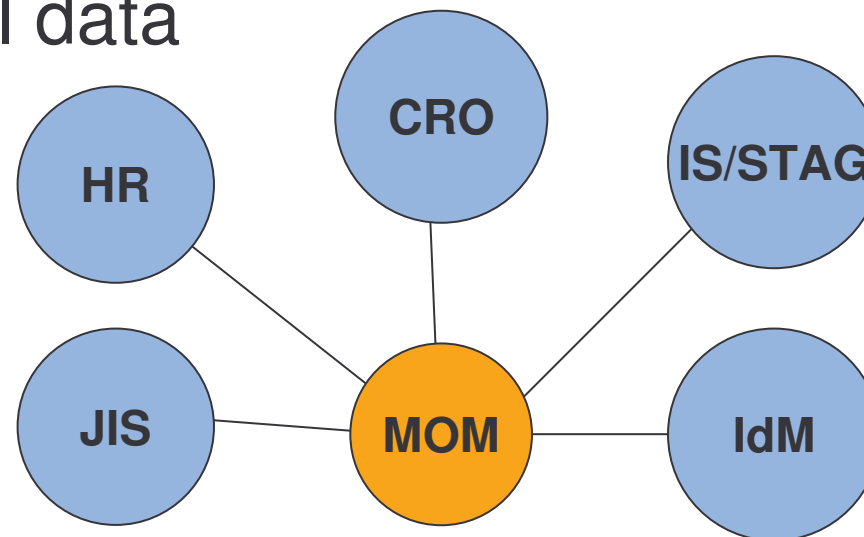
- Distributed computing environment at University of West Bohemia
- Based on open principles and technologies
- In operation since 1996
- Current ORION situation (approx. numbers)
  - 17000 users (5000 yearly amendments)
  - 6000 WEBnet workstations - 700 under ORION management
  - 180 servers
  - 50 centrally managed applications

# Goals of consolidating data sources

- Create a quality and credible source of identity data
- ORION main identity sources
  - students agenda (IS/STAG) - register of students and faculties
  - HR system (Magion) - register of employees and their affiliation
  - ORION computing system management (Moirá) - register of ORION users
  - identification card system (JIS) - electronic ID cards for students and staff

# CRO (Centralized Personnel Registry)

- Determine relationships between systems from personnel data perspective
- Testing communication infrastructure (Message Oriented Middleware)
- Define fundamental rules for sharing personnel data



# CRO data consolidation

- Goals: consolidate data from previously unrelated sources
- Automatic coupling of key items:
  - birth certificate number (social security number)
  - personal number
  - student number
- Manual processing
  - about 5 percent of identity records
  - in cooperation with departmental secretaries
- All took about six months

# Identity Management software features

- Quality provisioning (with least amount of changes to connecting systems)
- Simple workflow system
- Reasonable implementation cost
- Ability to connect to other systems using our own sources
- Vendor support, if needed

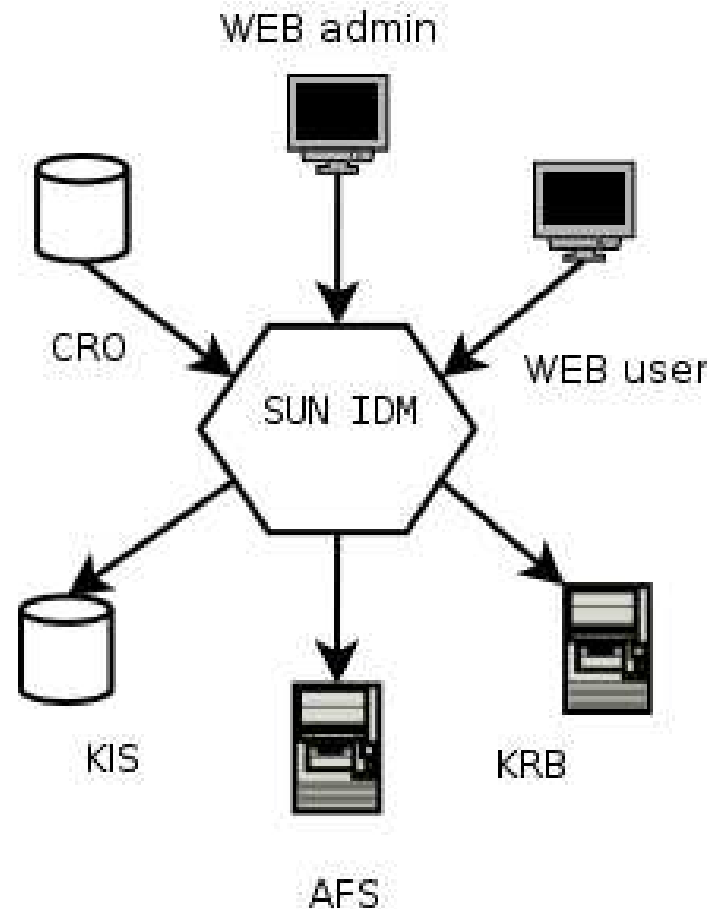
# Reasons for choosing Sun Java System Identity Manager

- Discharge of fundamental requirements
- Reasonable licensing fees
- User references
- Sun offer ORION a free Proof of Concept service
- Results of Proof of Concept



# ORION Proof of Concept components

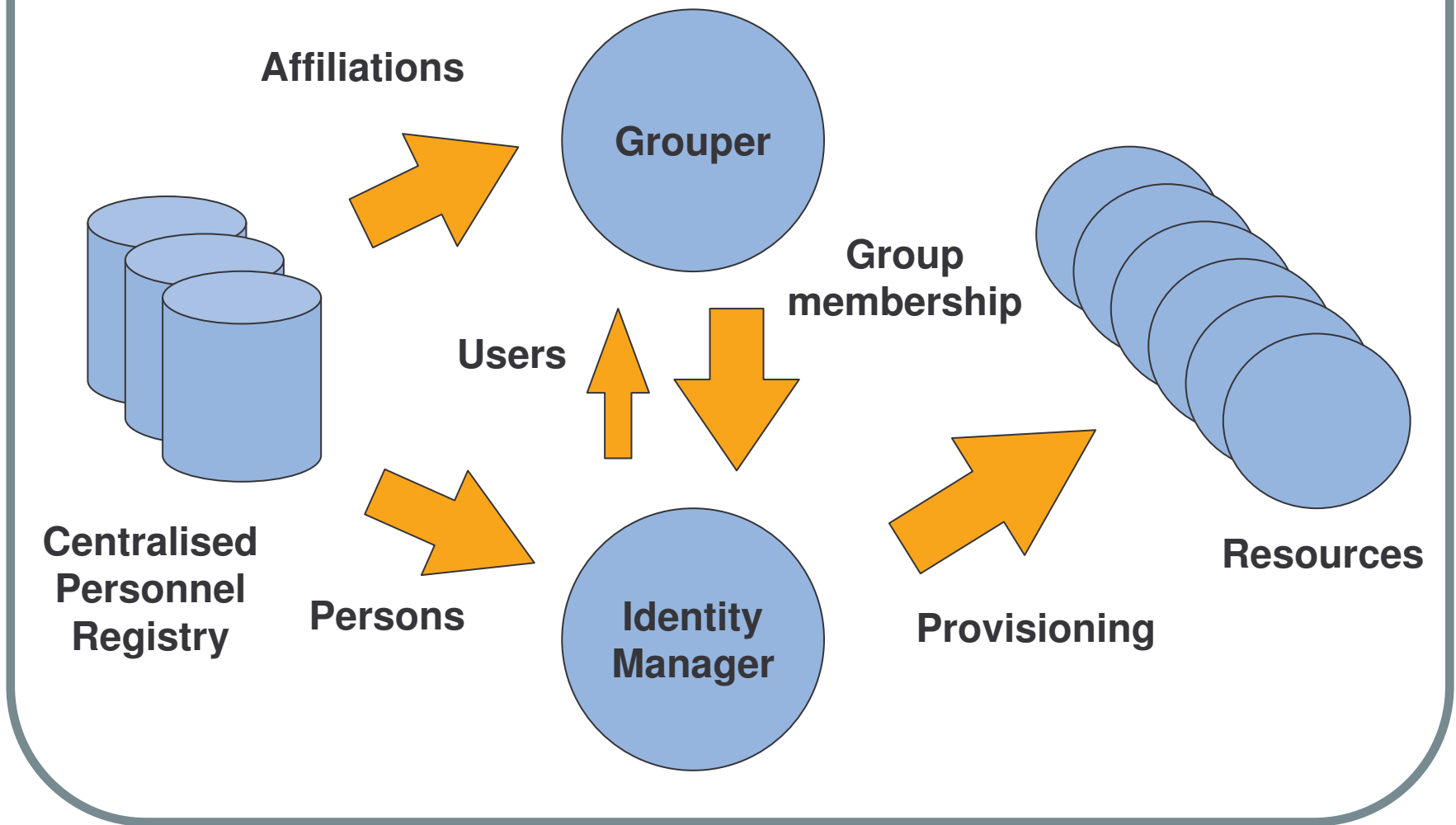
- Connection to Registry
- Web administration
- Web self administration
- Account lifecycle
- Typical application role assigning



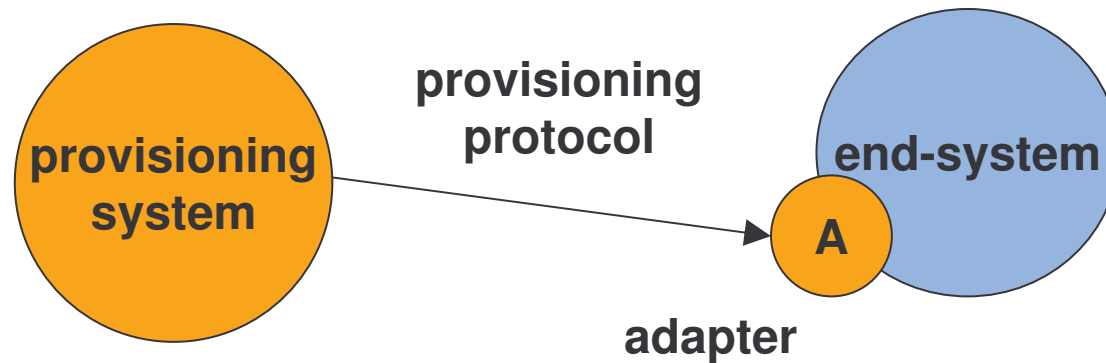
# ORION PoC results

- PoC requirements mostly proven
- Creating fundamentals for practical implementation of ORION Identity Management
- Necessity to supplement this solution with the Grouper system (Internet2 middleware project)

# ORION IdM scheme

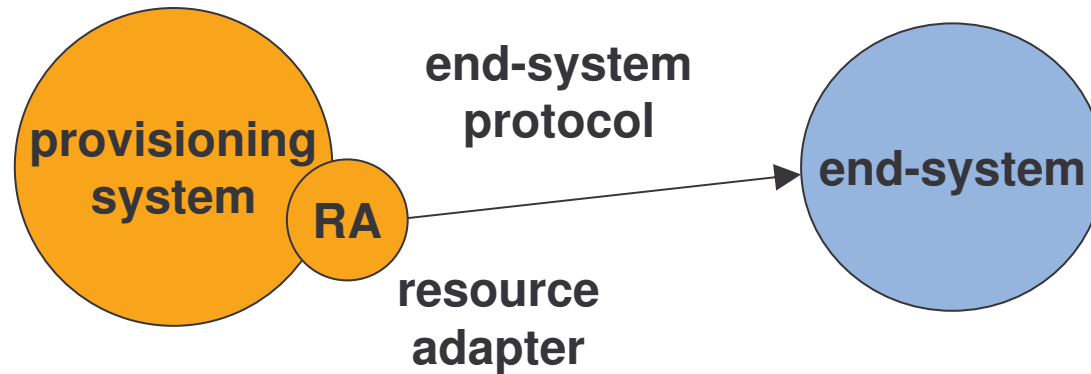


# Adapter provisioning



- specific communication protocol
- extra provisioning features allowed
- special adapter for each end-system needed

# Non-adapter provisioning



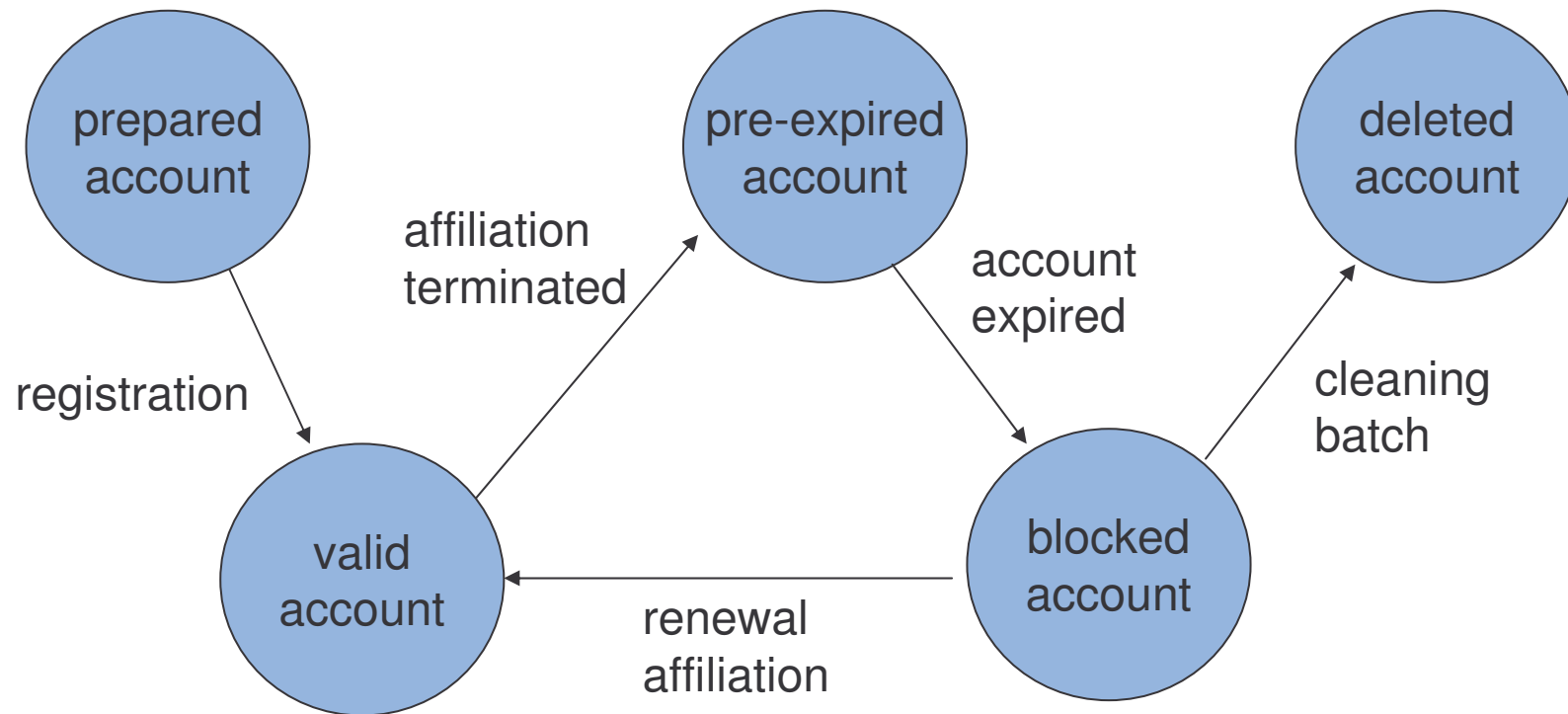
- no changes in end-systems needed
- simply connection to new end-system
- provisioning functions are limited by standard end-system protocol

# Roles and workflows

- Basic roles are implemented relatively easily
- Complete role system needs unified administrative processes within the organization
- Big number of main systems complicate role implementation
- Simple workflow system is sufficient in university environment

# Example of workflow

- Example of account life-cycle workflow



# Conclusions

- “To use or not to use” any particular IdM system
  - strong reason to justify big expense of implementation
    - we expect that new facilities bring large assets and/or
    - existing problems have to be evident and easily resolvable using IdM
  - “Trial and error” isn’t the answer



# Conclusions

- project timetable is expected to be fully operational by September this year
- existing project results
  - consolidated data in selected end-systems
  - revision of technology
  - procedural revisions
- Hopefully, we are going the right way

# Questions...

Thanks for attention

[borik@civ.zcu.cz](mailto:borik@civ.zcu.cz)