Identity Management in Advanced Education

Jens Haeusser
UBC

Lionel Tolar
SFU

Outline

- Overview of Business
- Current Infrastructure
- Short Term Activities
- Engaging Our Community
- Expanding Our Community
- Opportunities for Action

Our Challenge

- Identity Management within Advanced Education is highly complex and decentralized.
- Constant tension between our culture of openness and our need for privacy, while providing secure access to data.
- Federation is vital for our ongoing activities among our broad communities of interest

Overview of Business

- 100,000+ Students
- 20,000 Faculty & Staff
- $2 Billion Combined Annual Budget
- Learning
- Research
- Community Involvement

Overview of Business

- Universities are Municipalities
  - Sewer, Water, Power, Garbage, Transportation, Mail
  - Recreation, Hotel and Conference Facilities
  - Health Care, Dining, Retail Stores, Financial Service.
  - Community Internet

Campus Locations

Campus At Large

- High Availability ISP Services
  - Ubiquitous Network Connectivity
  - Collaborative Services – email, Web, Discussion Board, Instant Messaging, Blog, Wiki
- 100,000+ Active User Accounts
- 1 Million+ emails/day

Campus At Large

- Highly Secure IT Environment
  - Protect Intellectual Property
  - Protect Privacy
  - Protect Confidentiality
  - Protect Secrets

Students

- Student Information System
  - Airline Reservation System
- Online Learning Systems
  - WebCT, SAKAI, LON/CAPA, 1st Class, Moodle

Researchers

- Grant Tracking
- Patent Support/Legal
- Commercial Incubation
- High Performance Computing
- Massive Storage
- High Performance Network

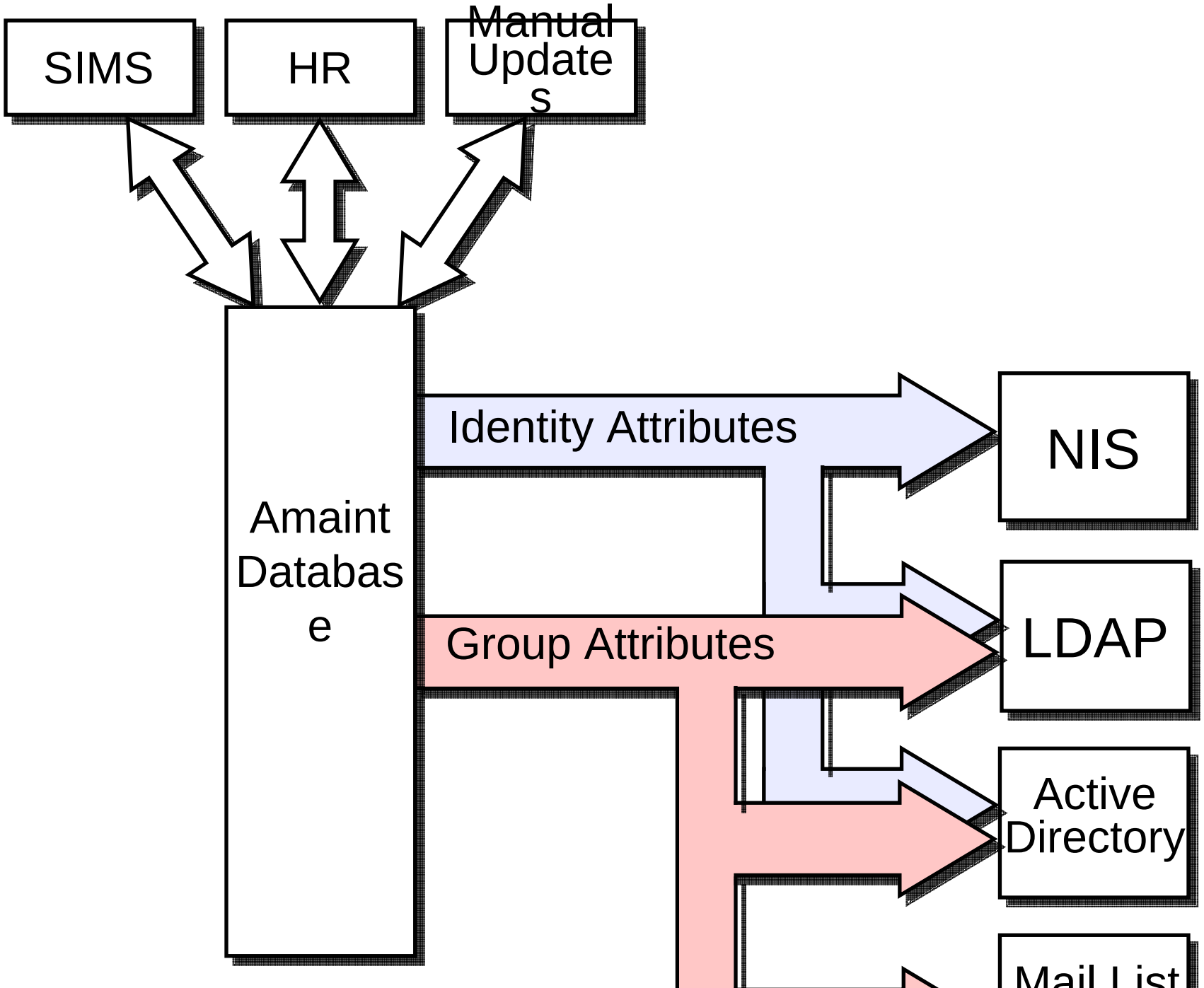
SFU IT Environment

- Infrastructure – SUN Solaris
- Administrative IT
  - ERP – PeopleSoft/DB2 on Solaris
  - Departmental Systems – Windows
- Research & Infrastructure
  - Open Source Clusters – HPC, Spam

Account Management

- Everybody has a central account.
- Single Sign-on available essentially everywhere.
- Identity assured by appropriate administrative entity. (HR, Registrar)
- Accounts issued when a user presents authorization and credentials.

Account Management



UBC IT Environment

- Extremely complex and decentralized
- Analogous to Provincial Government
  - Faculties ~= Ministries
- Central IT runs network, admin services
- Very heterogeneous (Sun/Linux/Windows)

UBC IT Environment

- Admin Systems:
  - HR/Finance - Peoplesoft
  - Student Information System - Homegrown
  - Oracle Database Backends
  - Many shadow account systems

UBC Account Mgmnt

- Web Initial Sign-On (CWL)
- User self-registration
- One-time validation vs Peoplesoft/SIS
- XML-RPC interface (JAVA APIs)
- Flexible but static role support

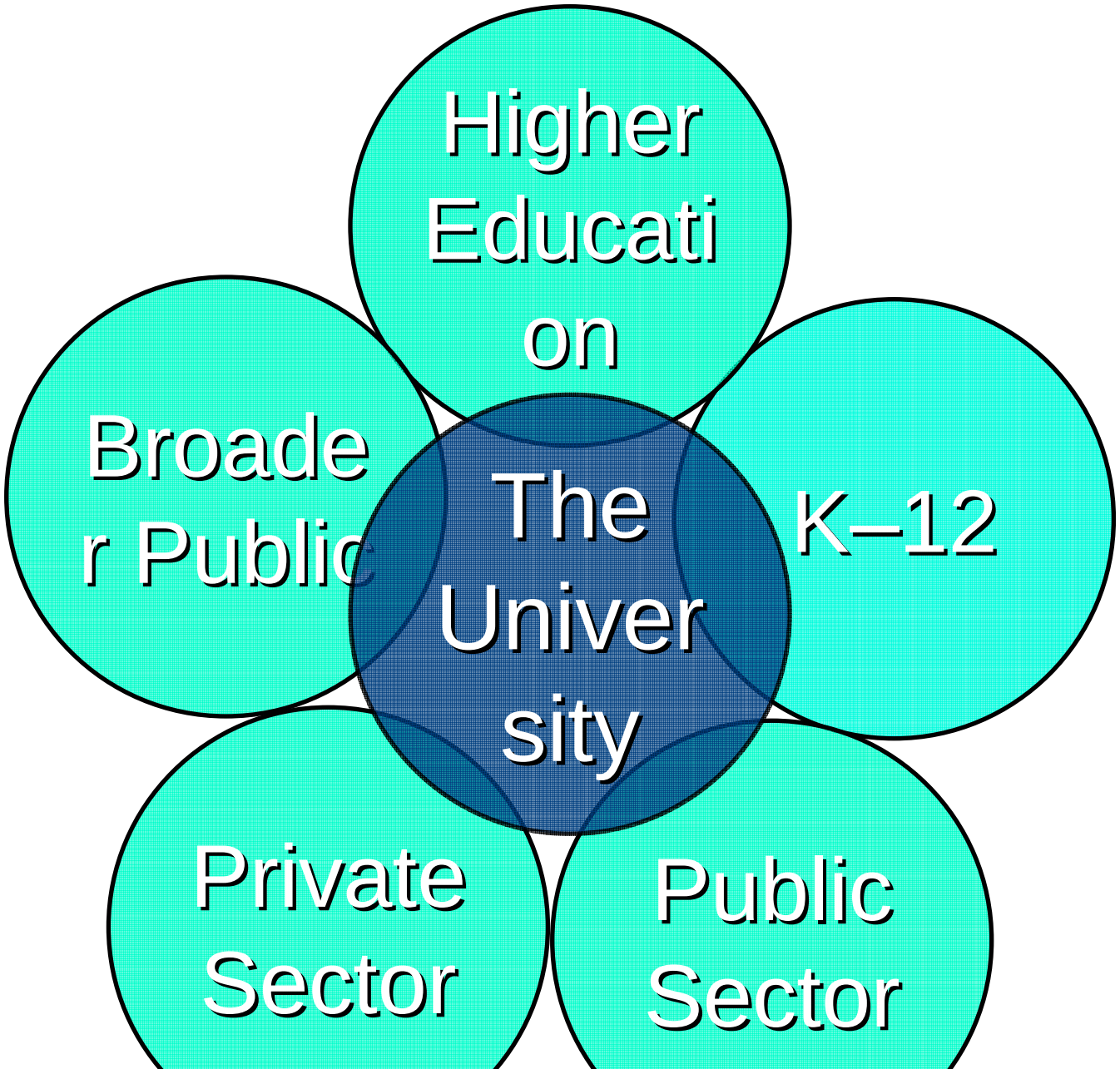
Short Term Plans

- Implement Sun Identity Management PoC
- Automated provisioning from Peoplesof
- Dynamic rule-based role assignment
- Standards-based interfaces for integration
- Distributed, delegated administration

Engaging Our Communities

- Access by anyone, from anywhere
- User-driven, self service
- Multiple, overlapping, evolving roles
- Cradle-to-grave identity
- Lifecycle management
- Require Federation, early and often

Communities of Interest



Expanding Our Community

- Implement Federated Identity Management Services to support collaborative requirements.
  - Simplify & Extend
  - Policy Foundation
    - Trust Framework
    - ID Assurance

Federation Technologies

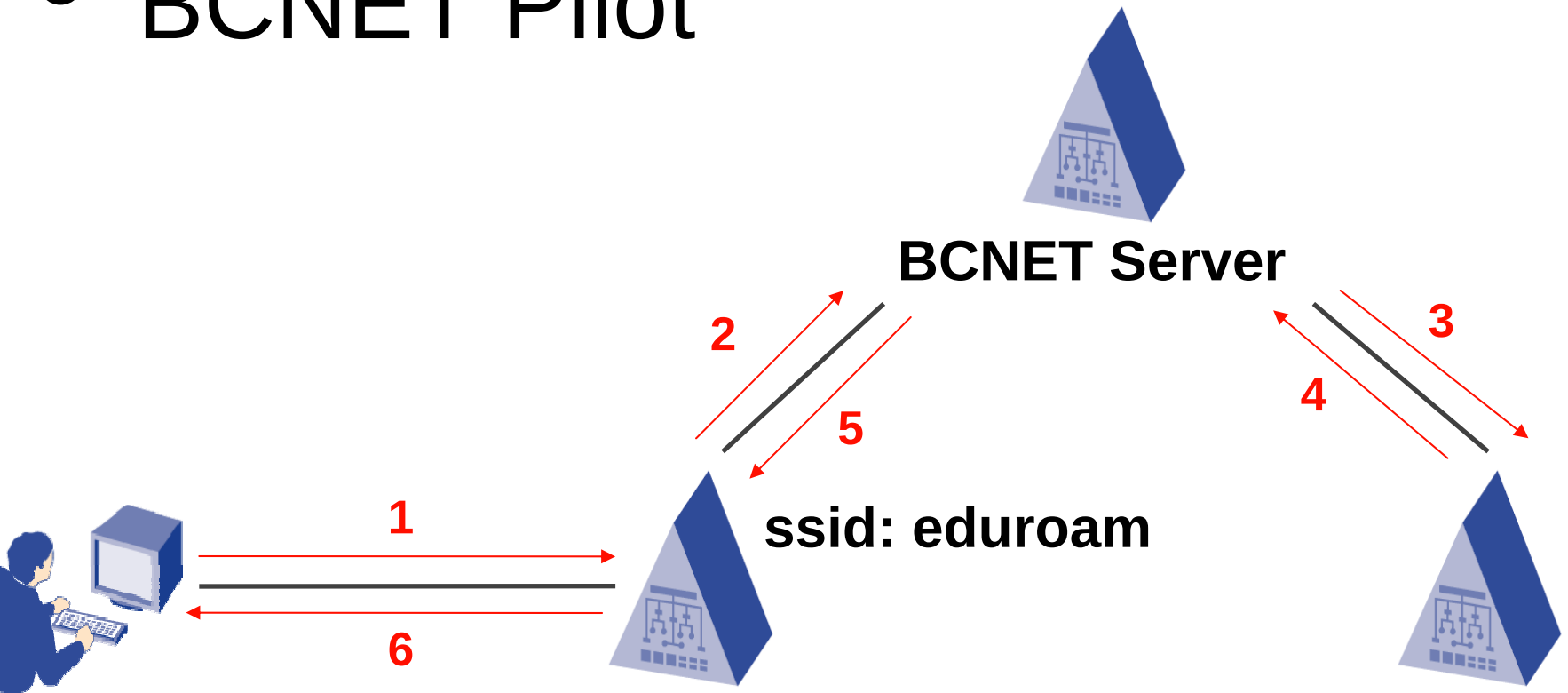
- Liberty-Alliance
- SAML
- WS-Trust
- WS-Federation
- Shibboleth
- Eduroam

- Open source inter-institutional web resource sharing
- Policy framework for higher-ed interoperability
- Currently based on SAML 1.1
- Ideal for lightweight web authentication
  - Digital libraries
  - Learning object repository

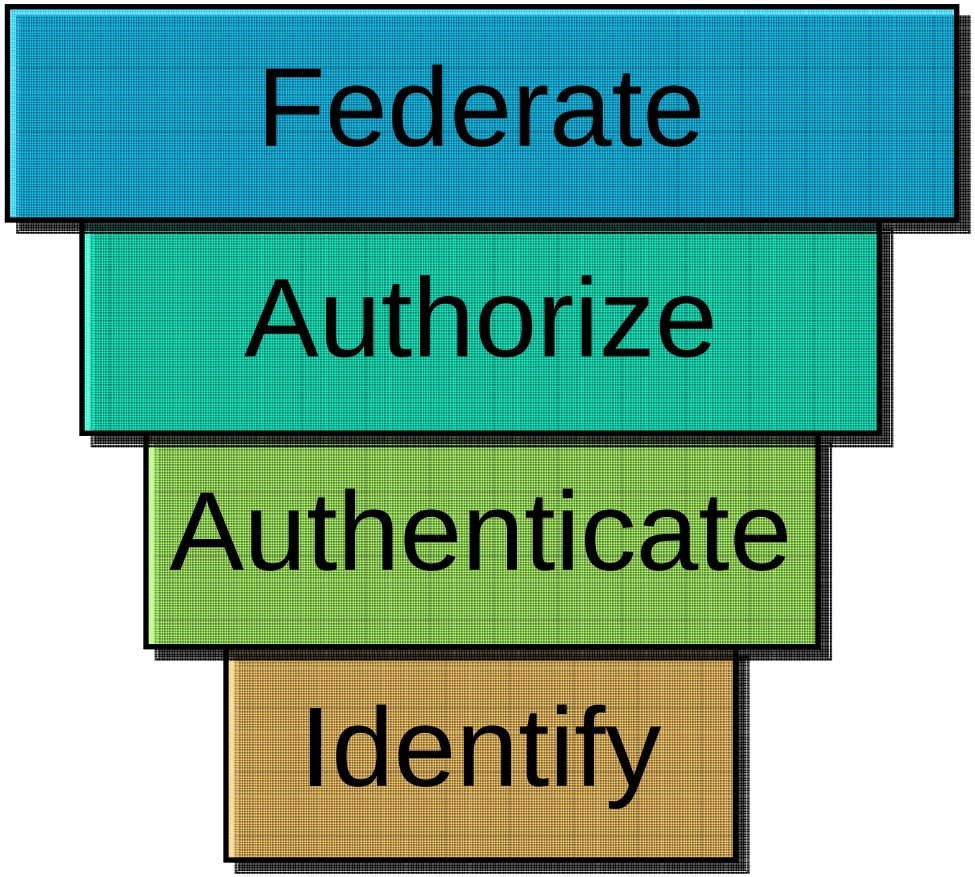
eduroam

Network roaming for higher education and research

- Inter-institutional wireless roaming
- RADIUS Proxy / 802.1x based
- BCNET Pilot



Identity Management Hierarchy



Trust Defined…?

- “We define trust as the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context.”
  - ***"Overview of Certification Systems: X.509, CA, PGP and SKIP", E. Gerc***

Trust Factors

- For two entities to trust each other they must have clear agreement for all of the processes, and attributes used to identify, authenticate and authorize an individual as well as the protocols used to communicate this information.
- Different entity relationships will require different agreements depending on their respective needs.

Trust Factors

- Federation**s...** not just Federation.
- We will utilize several federation agreements and utilize several federation protocols.
- Simple example agreement: http://www.eduroam.org/policy.php

Opportunities for Action

- Engage with our broad communities of interest and our public sector partners to deliver secure access to resources
- Enable research and secure collabouration with IDAM
- Leverage Federation to streamline access and foster cooperation between organizations

Questions? Comments?

- Lionel_Tolan@sfu.ca
- jens.haeusser@ubc.ca

- http://www.bc.net/applications/identity_management.htm
- http://www.it.ubc.ca/it/initiatives/Identity_Management.shtml
- http://shibboleth.internet2.edu/
- http://www.eduroam.org/