GTC

Identity Management: Who are YOU?

January 30, 2008

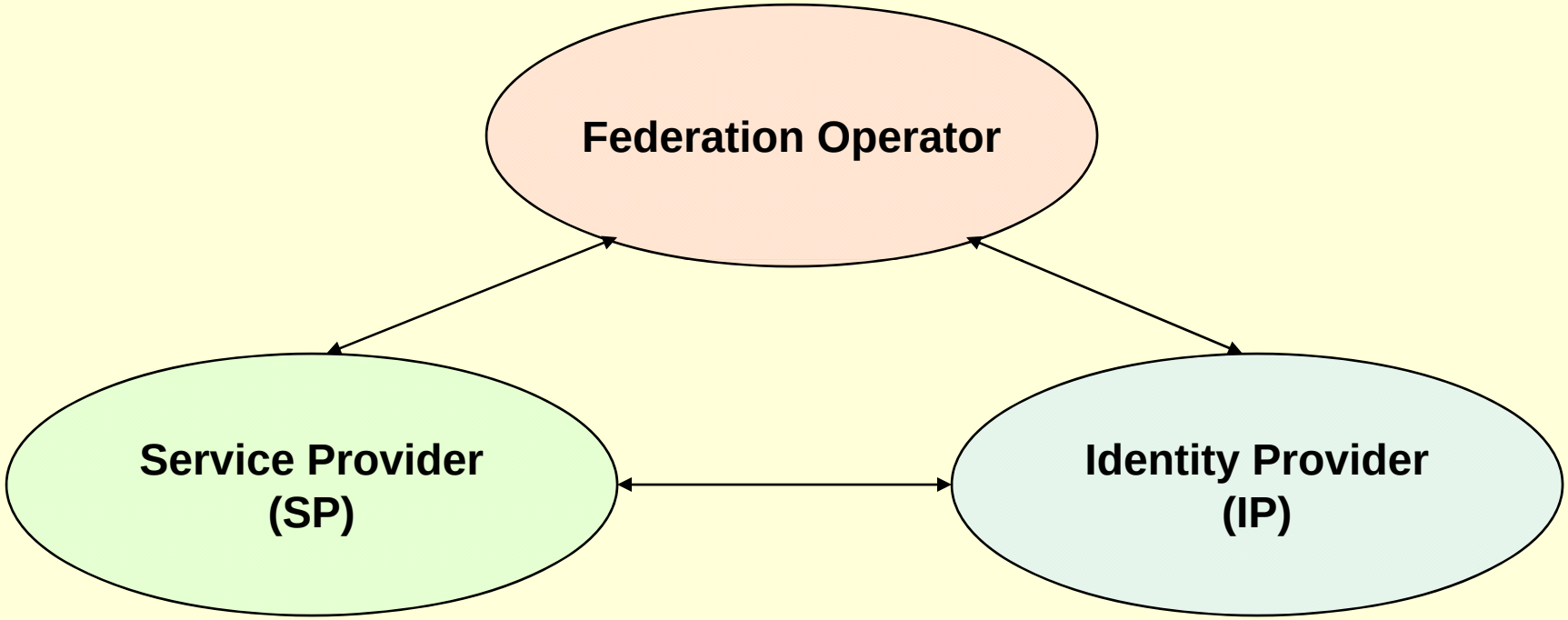
Clair Goldsmith

The University of Texas System

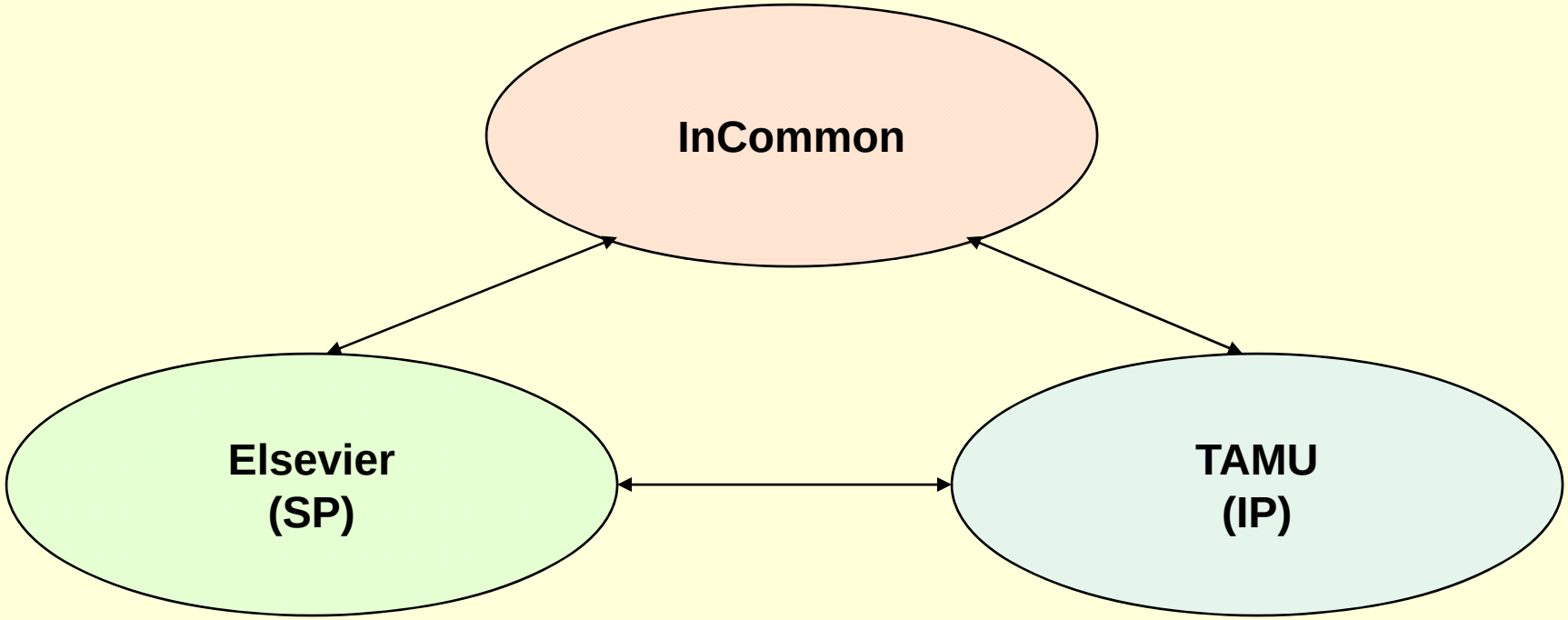
Definitions

- **Identity Management – the lifecycle of an identity**
- **Identity**
  - **A Label**
  - **May have associated attributes**
- **Authentication**
  - **Verification of identity owner**
- **Authorization**
  - **Capability assigned to identity**

Federated Identity Management

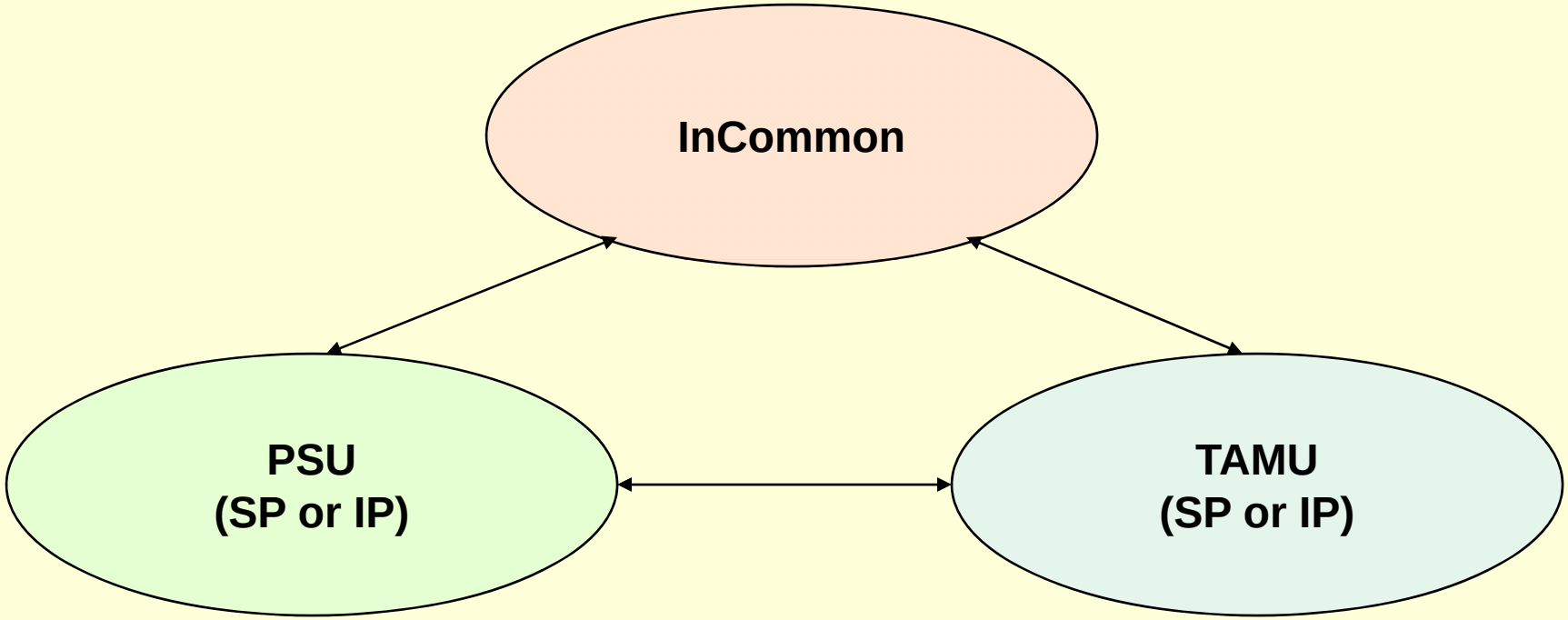


Federated Identity Management



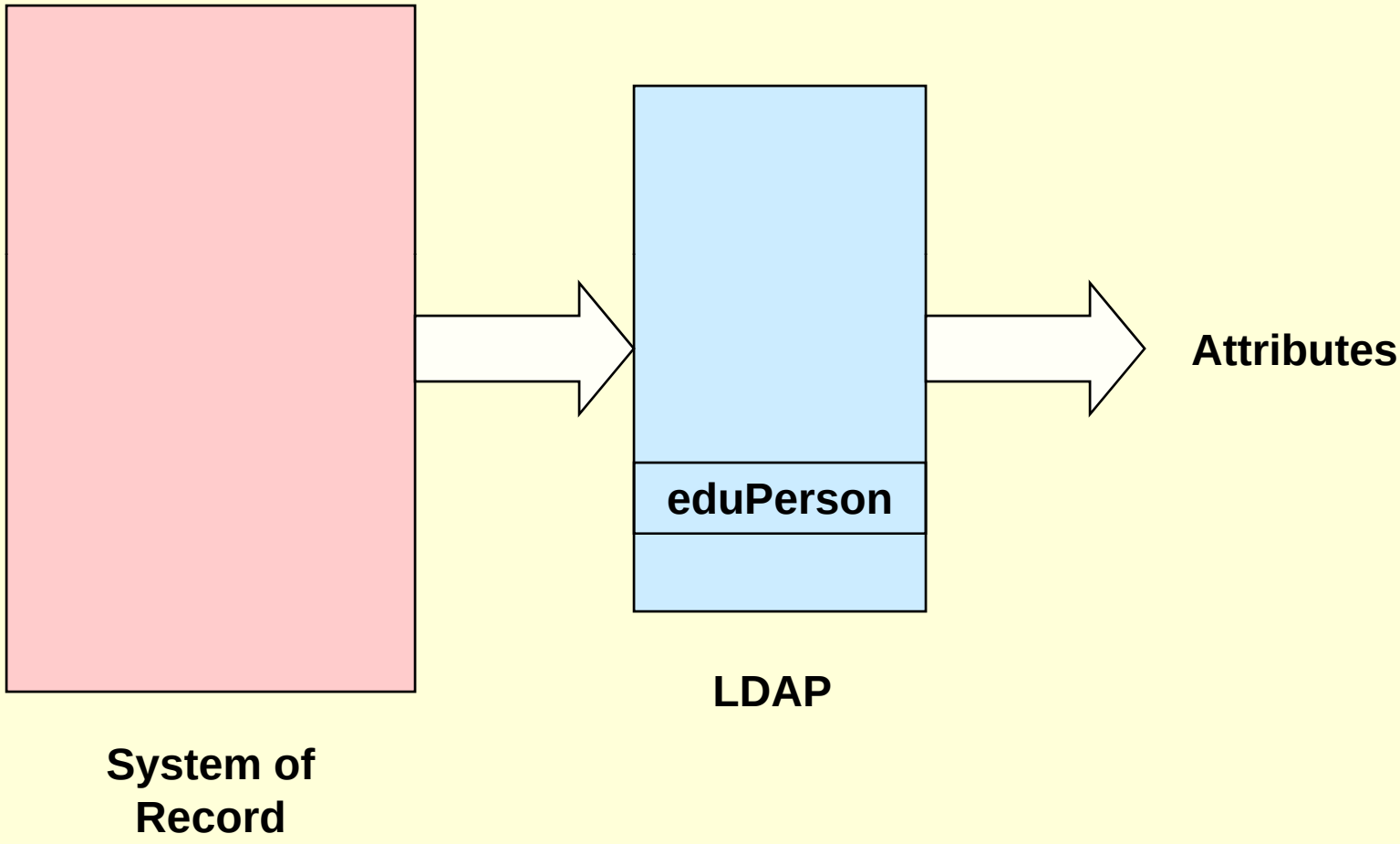
Automation of Trust

Federated Identity Management



Automation of Trust

Identity Management
Identity Provider

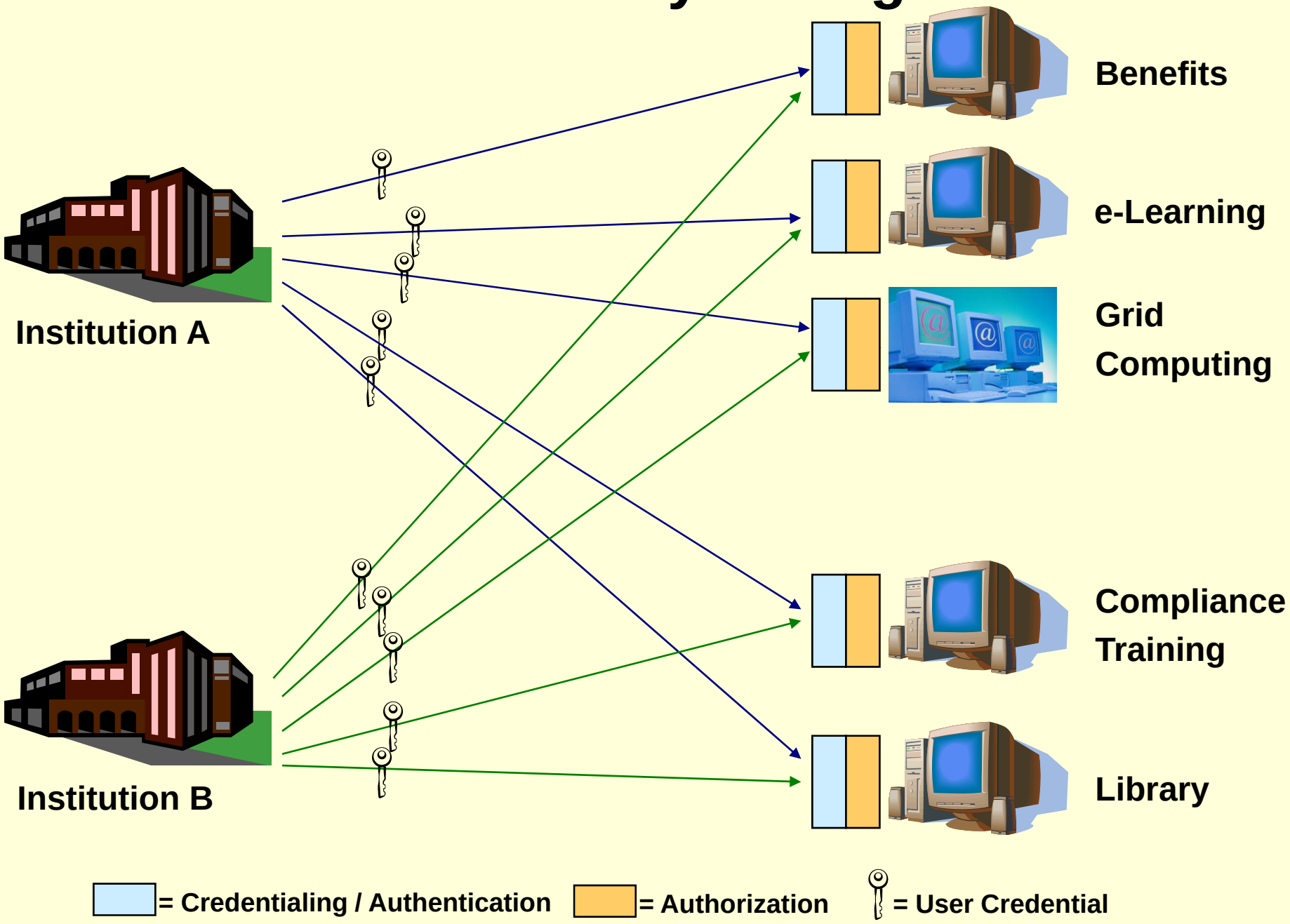


Why participate?

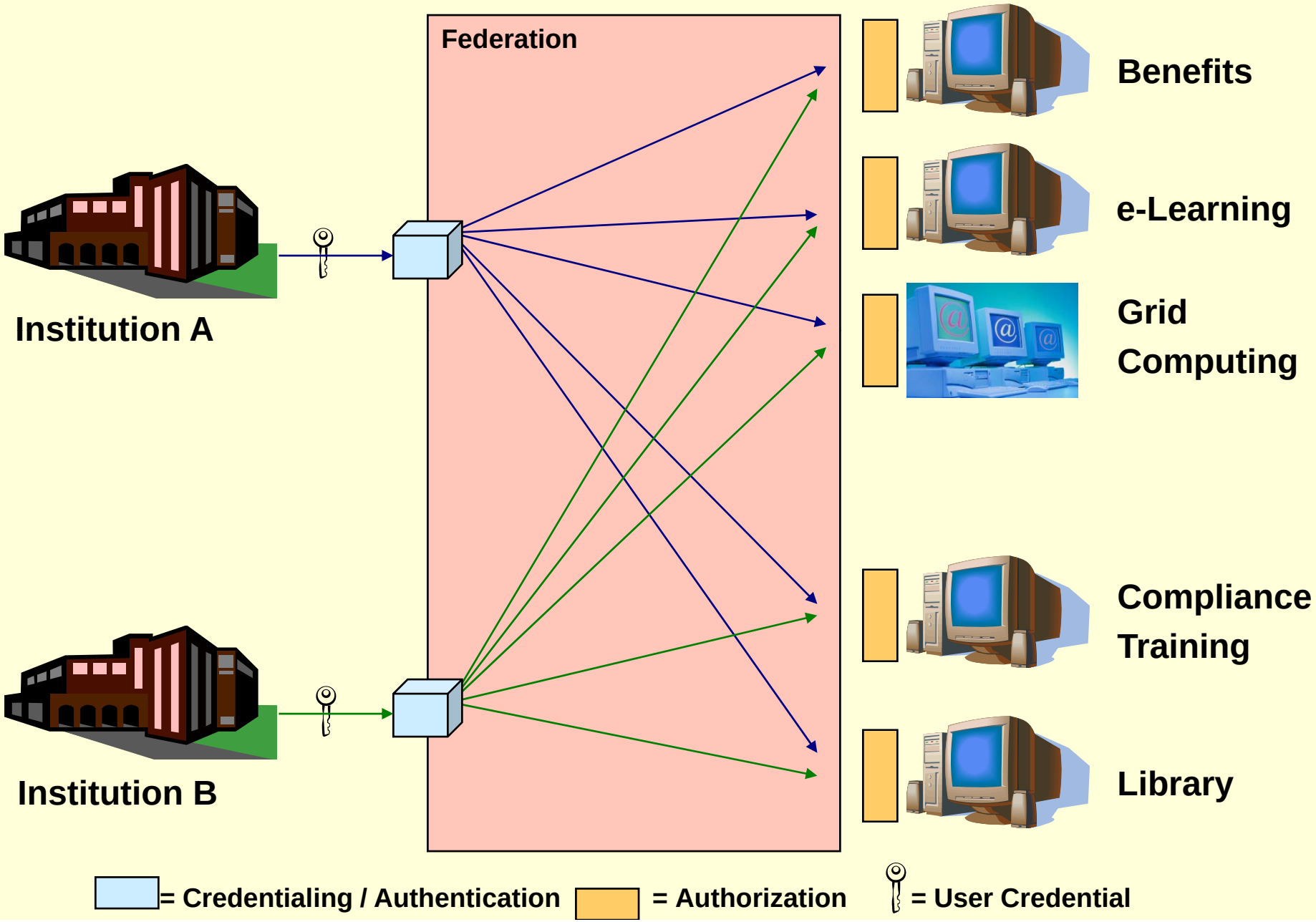
- **Scalable**
- **Secure**
- **Interoperable**
- **Trivial to share applications**
- **Reduced sign-on**

How Does It Work?

Traditional Identity Management



Federated Identity Concept



Components

1. **Technology**
   - **Known and available**
2. **Policy**
   - **Complicated and evolving**

Federations

- **InCommon -- Privacy Emphasis**
- **UT Identity Management Federation – Business Emphasis**
- **WS – FED**
- **OPENID**
- **DoD**

InCommon Members - 47

- California State University, Office of the Chancellor
- Case Western Reserve University
- Clemson University
- Columbia University
- Cornell University
- Dartmouth
- Duke University
- Florida State University
- Georgetown University
- Indiana University
- James Madison University
- Lafayette College
- Medical University of South Carolina
- Miami University
- Michigan State University
- New York University
- Northwestern University
- Ohio State University
- Ohio University
- Penn State
- Stanford University
- Stony Brook University
- Sweet Briar College
- Texas A & M University
- The Johns Hopkins University
- The University of Chicago
- University at Buffalo, SUNY
- University of Alabama at Birmingham
- University of California, Davis
- University of California, Irvine
- University of California, Los Angeles
- University of California, Merced
- University of California, Office of the President
- University of California, Riverside
- University of California, San Diego
- University of Maryland
- University of Maryland Baltimore County
- University of Maryland, Baltimore
- University of Massachusetts Amherst
- University of Richmond
- University of Rochester
- University of Southern California
- University of Virginia
- University of Washington University of Wisconsin - Madison
- Virginia Commonwealth University
- Virginia Polytechnic Institute and State University

InCommon SPs

- Cdigix
- EBSCO Publishing
- Elsevier ScienceDirect
- Houston Academy of Medicine - Texas Medical Center Library
- Internet2
- JSTOR
- NAS Recruitment Communications
- OCLC
- OhioLink – The Ohio Library & Information Network
- ProtectNetwork
- RefWorks, LLC
- Students Only Inc.
- Symplicity Corporation
- Thomson Learning, Inc.
- Turnitin
- WebAssign
- National Institutes of Health

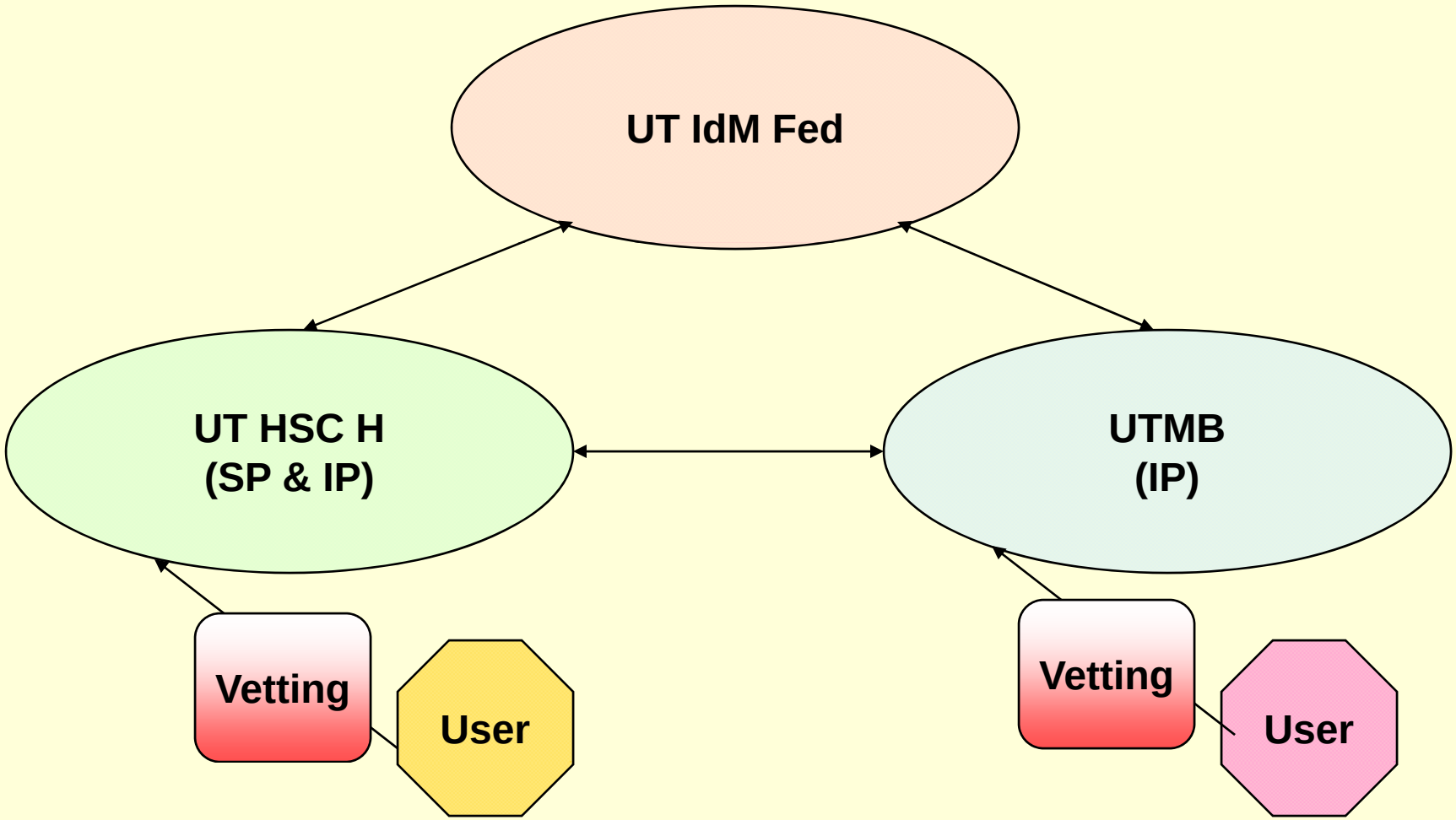
UT Federation

- Operational September 2006
- Signatories
  - UT MD Anderson
  - UT El Paso
  - UT Dallas
  - UT Medical Branch Galveston
  - UT System Administration
  - UTHSC Houston
  - UT Austin
  - UT Permian Basin
  - UT Tyler
  - UT HC Tyler
  - UT Pan American
  - UT Arlington
  - UTHSC San Antonio
  - UT San Antonio
  - UT Brownsville

Applications

- **All @ UT System Administration**
  - **Training, Financial Reports, etc. ~ 30 applications**
  - **All Fifteen Institutions**
  - **Guest Wireless for all UT institutions was first**
- **Blackboard @ UT HSC H**
  - **MD Anderson**
- **Research Collaboration @ UT Arlington**
  - **UT Dallas, UTSMCD**
- **FACN @ UT HSC H**
  - **UT HSC SA, UTMB, UTSMCD, *Texas Tech and TAMU in 2008***
- **MobileCampus @ MobileCampus (.com)**
  - **UT Austin, UT Arlington, UT Dallas, UT El Paso**

FACN Trust Issue



UT Federation

Why Will UT SPs and IPs trust each other?

- **Under a single Board?**
- ***Auditable* Agreements**

Future Applications

- **Student Information System as Shared Service in Arlington Data Center**
  - **UTA, UTD, and UTT**
- **Time & Effort in Houston Data Center**
  - **MD Anderson, UT HSC SA, UTMB,**
- **UT Austin Texas Advanced Computing Center**
  - **UT Institutions, TiGRE**
- **Cayuse for Five UT Institutions**
- **ISAAC**
- **Texas Digital Library (TDL) at UT Austin/TAMU**
  - **UT & TAMU, Rice, Tech, etc.**

UT Federation

- Uses Internet2 technology
  - Shibboleth
- Based on Standards and Best Practices
  - LDAP, eduPerson, SAML, etc
- Scalable, Secure, Interoperable
- Enabling Policies Exist
  - UT IdM Federation Documents
  - Based on InCommon policies and documents
- Governance Structure
- Business Emphasis

Related Efforts

- InCommmon/UT Fed
  - Inter-Federation
- Federal Government/UT Fed
  - Working with Federal PKI Bridge Policy Authority (NIH) on Cross Certification for higher levels of identity authentication assurance
    - Level 2 – in person vetting
    - Level 3 – two factor
    - Based on UT Fed MOP and Verisign CPS

What is Needed for Federated Identity Management Work?

- Technology Level – Not Much
- Policy Level – Most Work
  - Some Uncharted Territory
- Vision
- Policy
- Governance
- Plan
- Resources

Proposed LEARN Federation

- **LEARN education and Research Fiber Optic Network**
- **State agencies might also participate**

- **Vision**
- **Policy**
- **Governance**
- **Plan**
- **Resources**

What is Needed?

- **Vision**

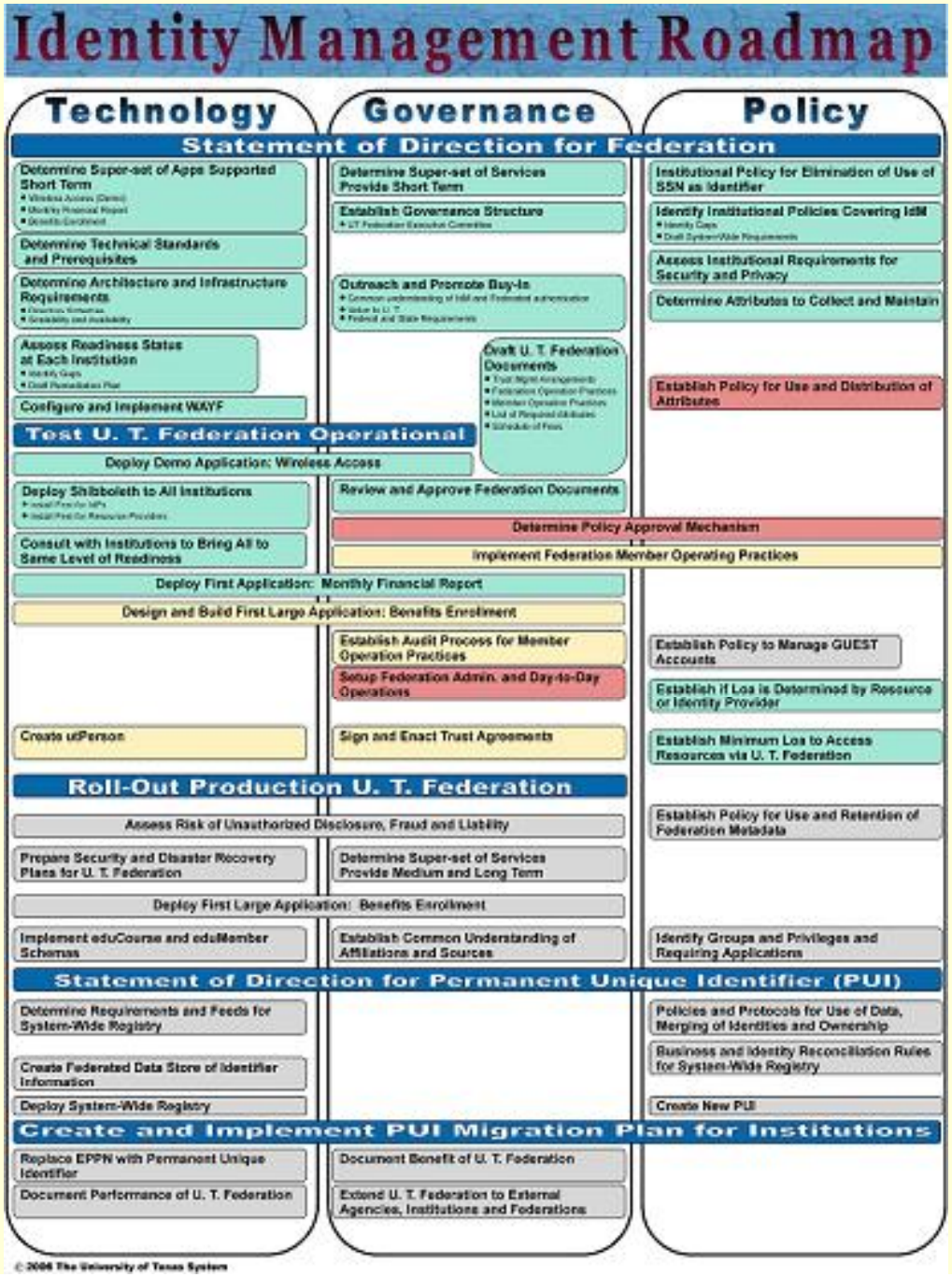
  All students, faculty, and staff of LEARN and its affiliates are able to access both local and remote resources using their local credentials and attributes, through a seamless technology infrastructure.

What is Needed?

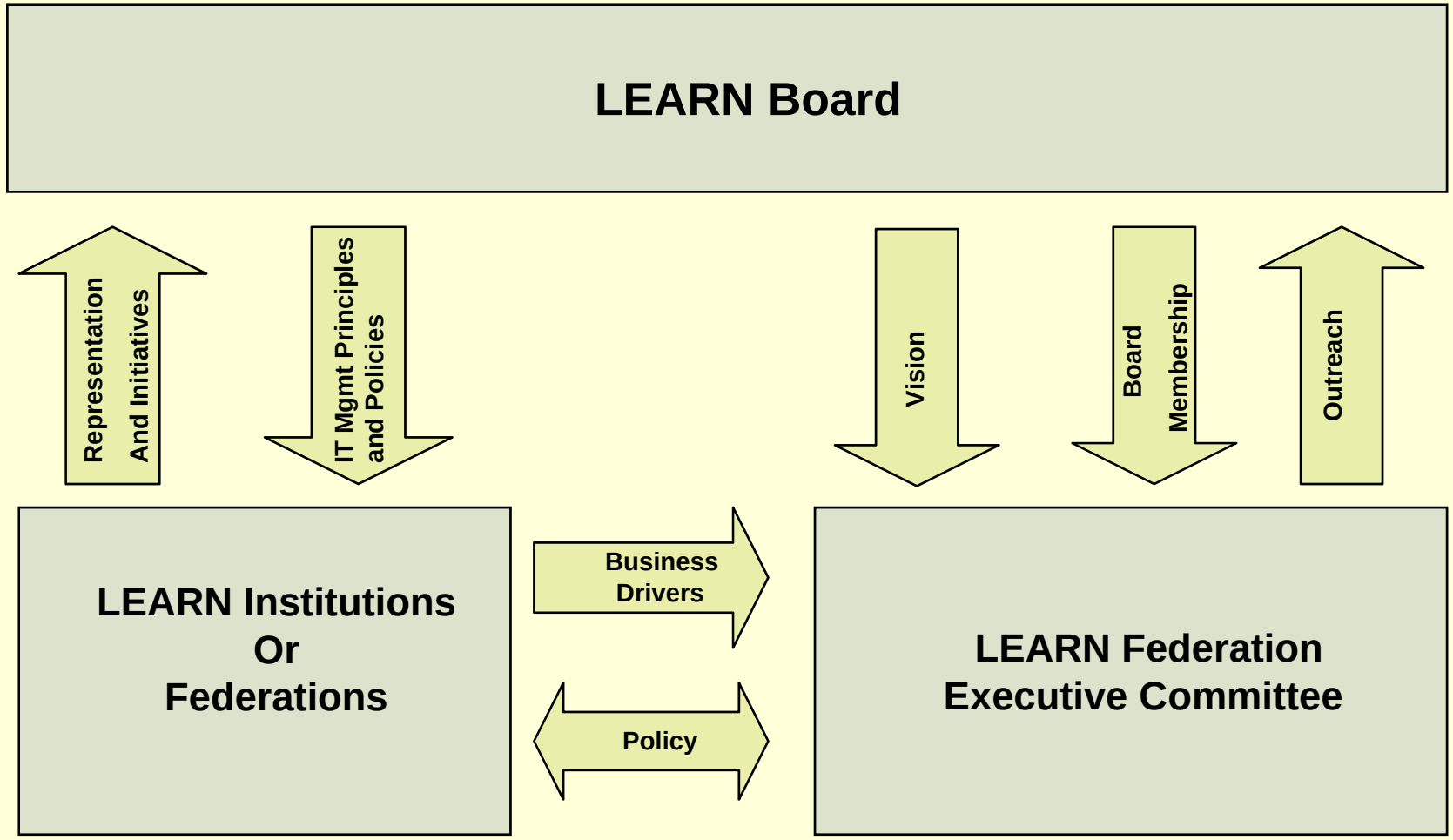
- **Vision**
- **Business Drivers**
  - **Build Identity Management infrastructure to enable greater synergy and collaboration among LEARN institutions and state agencies**
  - **Application security simplified thru common trust fabric, allowing the secure exchange of identity authentication and authorization attributes**
  - **Implement a common framework, standards and protocols, for attribute naming, storage, and exchange (LDAP, eduPerson, SAML)**

What is Needed?

- **Vision**
- **Business Drivers**
- **A Plan**



LEARN IdM Federation: Governance



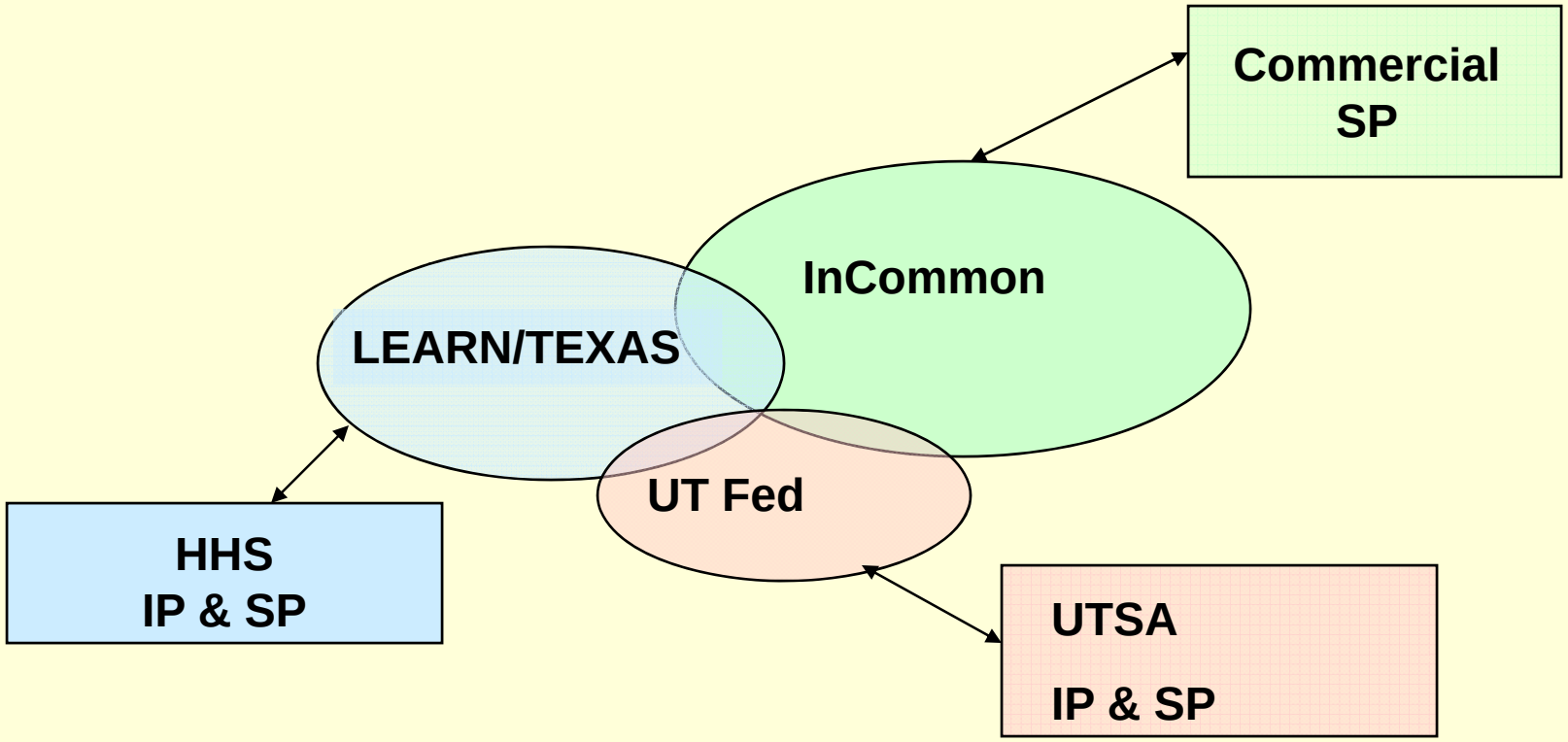
LEARN IdM Federation: Policy Documents

- ✓ Use InCommon as model
  - ✓ Federation Charter
  - ✓ Federation Operating Practices
  - ✓ Membership Operating Practices *(Different from InCommon)*
    - Explicitly defines standards, policies and procedures that federation members must put in place to be able to make real, informed relying party decisions
    - Use University of California UCTrust Federation document as format
  - ✓ Membership Agreement *(Different from InCommon)*
    - Leverage existing inter-institution LEARN membership document to simplify membership contract
  - ✓ Federation Attribute Table
  - ✓ Membership Fee Schedule

Issues

- **The Technical implementation of the Federation can outpace Policy and Governance**
- **Governance entangled with power/autonomy conflicts**
  - **Priorities vary by institution/agency**
  - **Conventions may be seen as dictates**
- **Managing trust relationships is complex when dealing with institutions within the same family. Complexity increases as diversity of membership increases**

The Future: Inter-federation



-This Works Today

-Technology Exists

-Policy Does Not Exist

Potential Applications

- **CTSA**
- **caBIG and State Funded Cancer Research**
- **Dynamic network provisioning**
- **And 100s more…**

References

- **UT System Identity Management**
  http://idm.utsystem.edu/utfed/
  See last five lines for links to the documents.
- **InCommon**
  http://www.incommonfederation.org/
- **Federated Identity**
  http://en.wikipedia.org/wiki/Federated_identity

Thank You

cgoldsmith@utsystem.edu