InCommon®

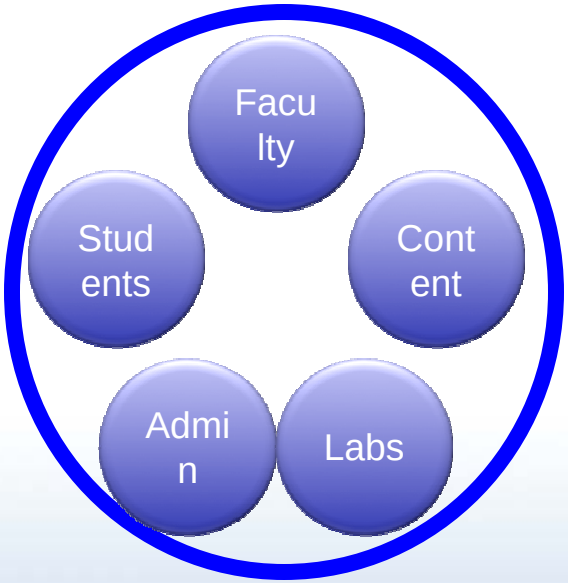
The InCommon Federation

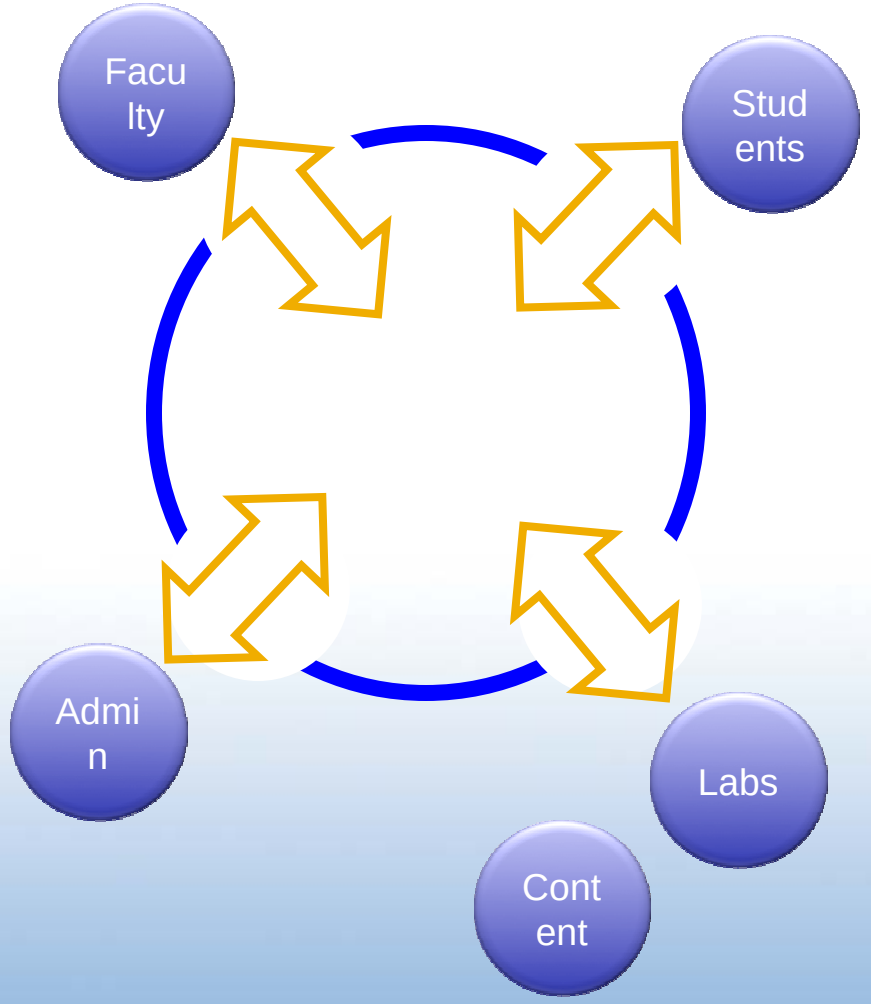
The U.S.
Identity and Access Management
Federation
for Higher Education and its Partners

www.incommon.org

InCommon®

Central ---> Distributed





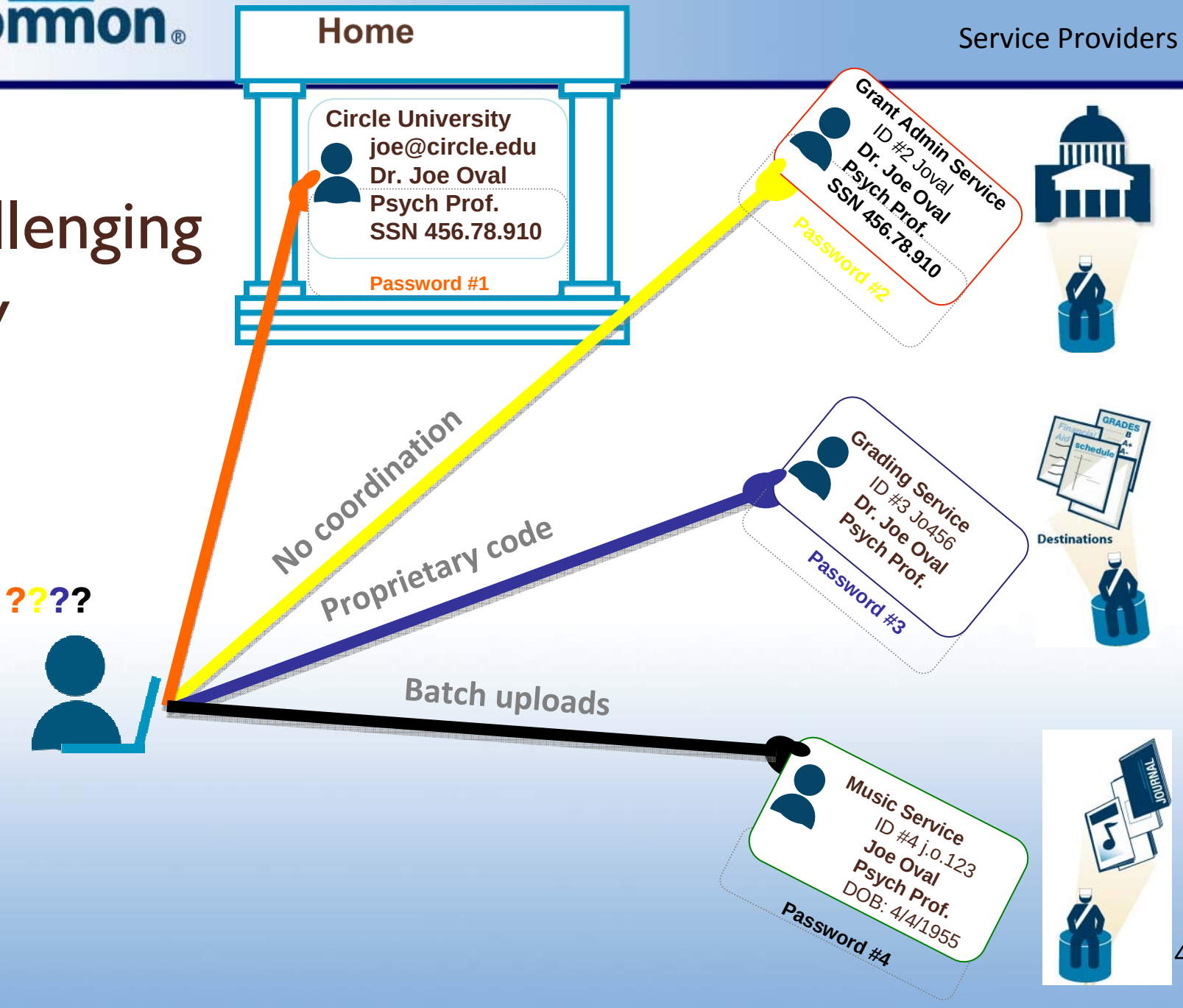
InCommon®

Distributed System Problems:

- Information flows of identity: Exposure, Theft
- Unmanageable number of credentials
- Complexity of implementation for central IT
- Increased help & support
- How many off-campus applications do you have?
- How do these service providers
  - Verify the identity of your students?
  - Know who's eligible to access the service?
  - Know the student is active and hasn't left school?
- How comfortable are you with the security and privacy of the identity data?

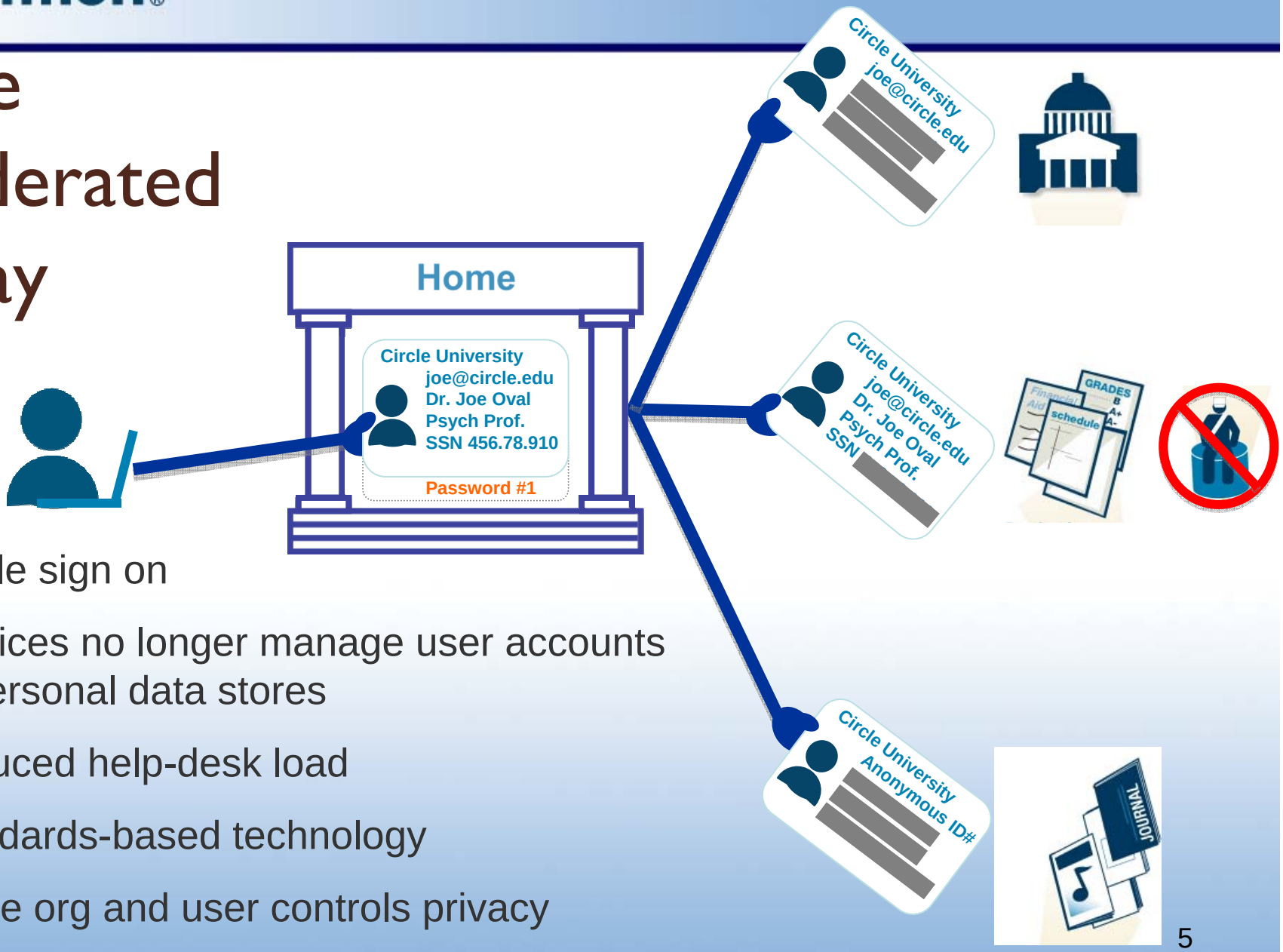
InCommon®

The Challenging Way



InCommon®

The Federated Way



1. Single sign on
2. Services no longer manage user accounts & personal data stores
3. Reduced help-desk load
4. Standards-based technology
5. Home org and user controls privacy

InCommon®

A Screen Capture Example

http://people.internet2.edu/~jcwk/Multiple_SPs_IdPs/Multiple%20SPs%20IdPs.html

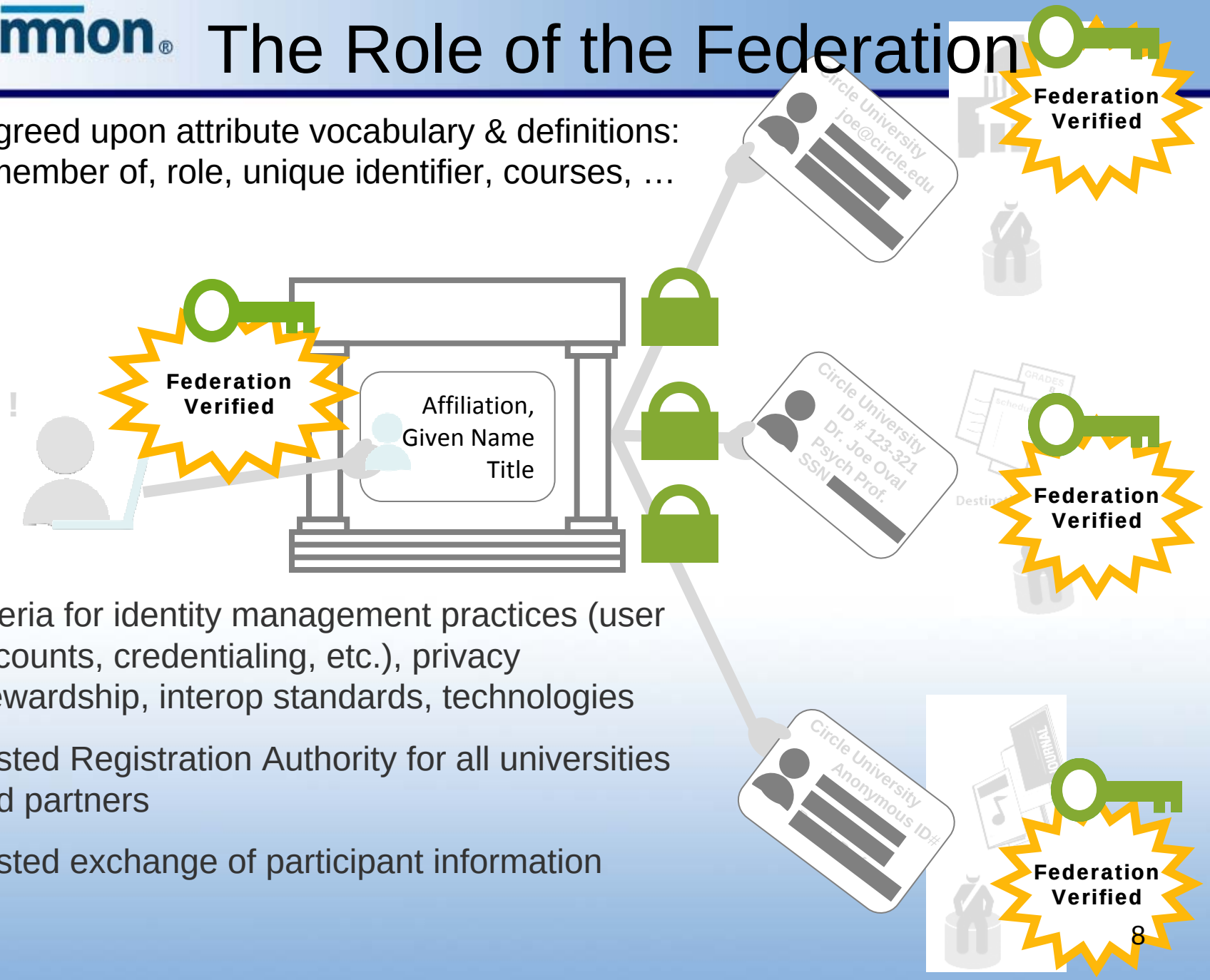
InCommon®

SAML, Shibboleth, EduPerson

- Security Assertion Markup Language (SAML)
  - Standard for the formation and exchange of authentication, attribute, and authorization data as XML.
- Shibboleth Single Sign-on and Federating Software
  - Open source software uses SAML to perform this exchange across boundaries
- EduPerson schema for attributes, identity and affiliation information

The Role of the Federation

1. Agreed upon attribute vocabulary & definitions: member of, role, unique identifier, courses, …



2. Criteria for identity management practices (user accounts, credentialing, etc.), privacy stewardship, interop standards, technologies
3. Trusted Registration Authority for all universities and partners
4. Trusted exchange of participant information

InCommon®

Federations: Who's Using This Approach?

- Higher-Education Systems
  - U of TX, U of CA, Cal State U, Indiana, U of MD, Missouri, …
- Network Providers
  - NJEdge, MCNC (North Carolina), Great Plains Network…
- National
  - UK, Switzerland, The Netherlands, Sweden, Norway, Denmark, France, Germany, Australia… and US

InCommon®

Federations: Why?

- Minimizing distribution of PII
  - Pass only what's needed for access
  - Privacy can be maintained
- Service tied to role and affiliation status
  - Changes affect access: Security
- Ease of use
  - SSO for on- and off-campus services
  - Timely access
- Time and money savings
  - Use of the same technologies and standards for each service partner

InCommon®

Federated Value for Universities

- "… we conservatively estimate that we save $85K per federated application (does not include power and cooling savings). With 10 federated applications, that's $850K annually. These are just the central IT cost savings and do not include what we know to be reduced support costs, which are impossible to capture. In our first production app, an 80% reduction in help desk calls was measured between semesters due to password resets."
  - Research university CIO, September 2009

InCommon®

InCommon Federation

- US Research and Education Federation
  - www.incommon.org
  - LLC operated by Internet2 with separate governance
- 185 participants representing over 3 million individuals.
- Agree to a common participation rules that allows each to interoperate with the others
  - Sets basic practices for identity providers and service providers

InCommon®

InCommon Identity Assurance

- Specifies criteria used to assess the credential strength of identity providers:
  - InCommon Bronze and Silver Identity Assurance Profiles
- Provides initial practices for authentication processes and technology
- Based on foundational Government Standard: NIST 800-63 Electronic Authentication Guideline

InCommon®

InCommon Activities

- Collaboration
  - InC-Library, InC-Student, InC-NIH, InC-Research, InC-Apple, Dreamspark, Microsoft Server Platform (Geneva)
- National and International standards
  - Co-wrote SAML spec
  - Involved in WS-Fed, OASIS, Terena, ISOC, and Liberty Alliance and other standards and federation organizations
  - Working with PESC
- Development Work
  - Interfederation, Privacy and Consent, Evolution of Federations