

Federations and InCommon

The Problem

- ▶ Scaling
- ▶ Service management
- ▶ Authentication by identity holder
- ▶ Authorization by service provider
- ▶ Security and privacy
- ▶ Accuracy and timeliness

What does a Federation do?

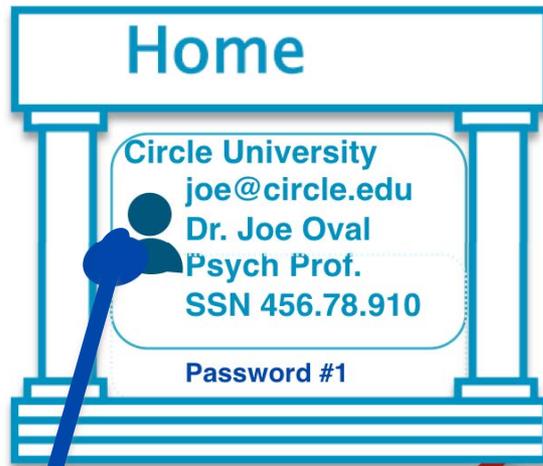
- ▶ Scaling beyond the technology
 - Rules of Engagement
 - Information about how to connect
- ▶ Vetting organizations and representatives
- ▶ Common Data/Attribute
- ▶ Shared Technology
- ▶ Maintain Member Information

The Challenging Way

Home

Circle University
joe@circle.edu
Dr. Joe Oval
Psych Prof.
SSN 456.78.910

Password #1



Service Providers

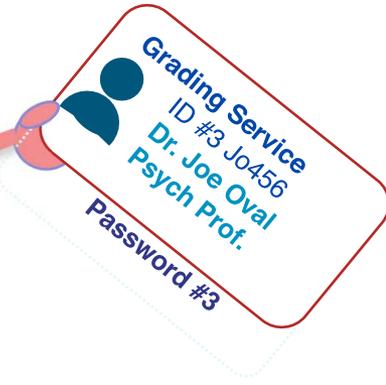
Grant Admin Service
ID #2 Joval
Dr. Joe Oval
Psych Prof.
SSN 456.78.910

Password #2



Grading Service
ID #3 Jo456
Dr. Joe Oval
Psych Prof.

Password #3



Music Service
ID #4 j.o.123
Joe Oval
Psych Prof.
DOB: 4/4/1955

Password #4



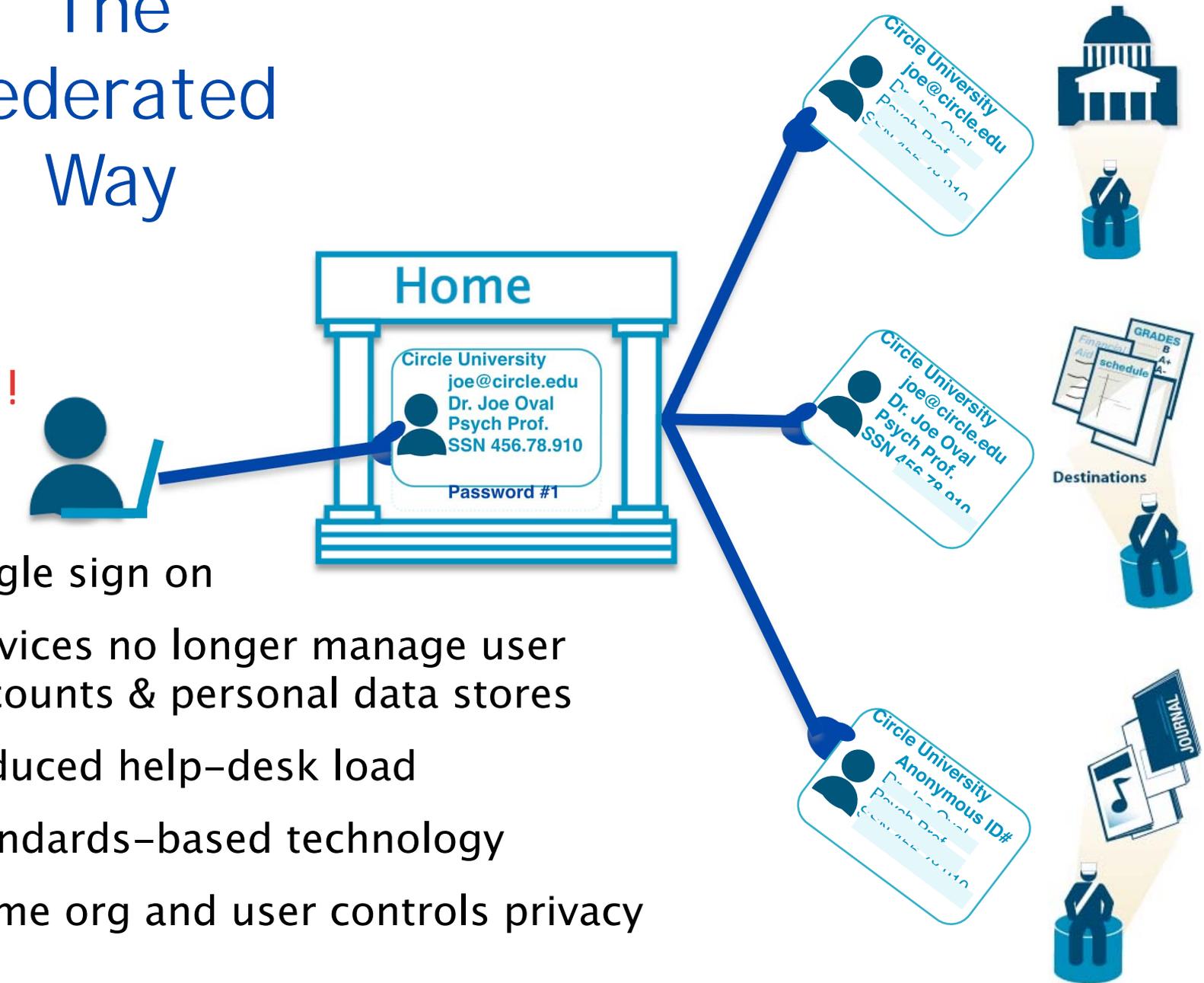
No coordination
Proprietary code

Batch uploads

?????



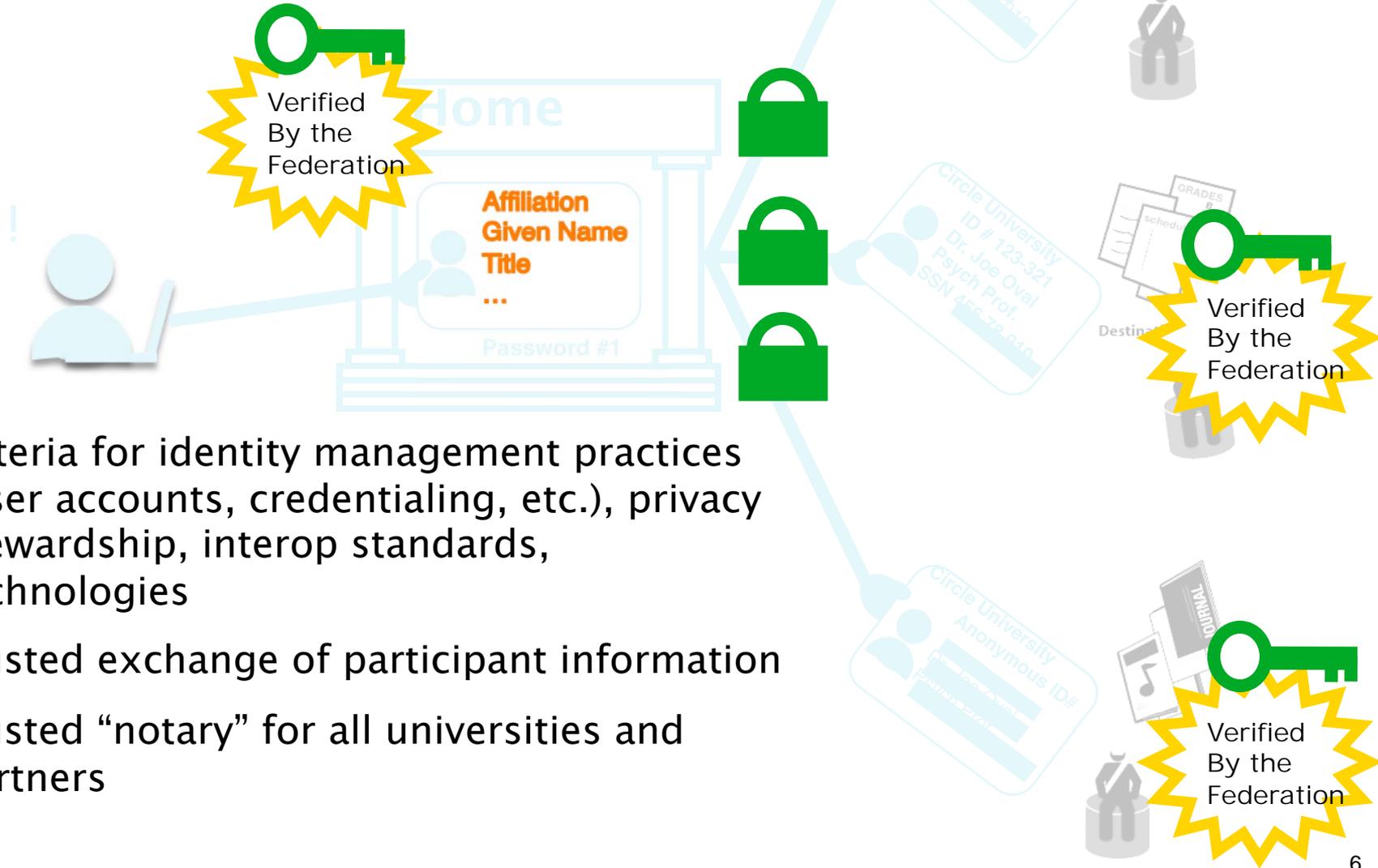
The Federated Way



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

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 exchange of participant information
4. Trusted “notary” for all universities and partners

Federation Metadata

-    **College A**
IdP: name, key, url, contacts, etc.
SP1: name, key, url, contacts, etc.
SP2: name, key, url, contacts, etc.
-   **University B**
IdP: name, key, url, contacts, etc.
SP1: name, key, url, contacts, etc.
-    **University C**
IdP: name, key, url, contacts, etc.
-   **Partner 1**
SP1: name, key, url, contacts, etc.
-    **Partner 2**
SP1: name, key, url, contacts, etc.
SP2: name, key, url, contacts, etc.
-    **Partner 3 ...**

InCommon
Federal
Compliant
Assurance
Levels

Verified
By the
Federation

Verified
By the
Federation

Verified
By the
Federation

InCommon Federation

- ▶ US Research and Education Federation
 - www.incommon.org
 - Separate entity with its own governance
 - Operations managed by Internet2
 - Members are degree granting accredited organization and their partners

InCommon Steering Committee

Steering Committee

Lois Brooks, Stanford University –
Chair

Kevin Morooney, Penn State –
Vice chair

Steve Cawley, University of
Minnesota

Joel Cooper, Carleton College

Clair Goldsmith, University of
Texas System

Ken Klingenstein, Internet2 (ex
officio), University of Colorado

Tracy Mitrano, Cornell University

Chris Shillum, Elsevier

Jack Suess, University of Maryland,
Baltimore County

Mike Teets, OCLC

Advisors

Renee Frost, Internet2,

University of Michigan

Norma Holland, EDUCAUSE (ex
officio)

David Wasley, retired, UCOP

Role

Manages the business and affairs of InCommon and its Federation, including oversight and recommendations on issues arising from the operation and management of the InCommon Federation.

InCommon Technical Advisory Committee

RL "Bob" Morgan, University of Washington - Co-Chair

Renee Shuey, Penn State - Co-Chair

Tom Barton, University of Chicago

Scott Cantor, The Ohio State University

Steven Carmody, Brown University

Paul Caskey, University of Texas System

Michael Gettes, MIT

Keith Hazelton, University of Wisconsin - Madison

Ken Klingenstein, Internet2/
InCommon Steering Committee

Mike LaHaye, Internet2

David Walker, University of California-Davis

David Wasley, retired, UCOP

Role

Provides recommendations relating to the operation and management of InCommon with respect to technical issues.

InCommon Members

- ▶ Presently about 124 members, approximately 81 higher education institutions, 5 government agencies or non-profit laboratories, and 33 corporations (public and non-profit) representing 2.2 million individuals.
- ▶ Entities agree to a common participation agreement that allows each to inter-operate with the others.
- ▶ InCommon sets basic practices for identity providers and service providers. The primary focus has been technical and focuses on campus identity management procedures and attributes.

InCommon Activities

Collaboration

- InC–Library, InC–Student, InC–NIH, InC–Research, InC–Apple, Microsoft Dreamspark

National and International standards

- Co–wrote SAML spec
- TAC members involved in WS–Fed, OASIS, Terena, ISOC, and Liberty Alliance and other standards and federation organizations

Development

- Interfederation, Privacy and Consent, Evolution of Federations

Joining InCommon

Management Process

1. Eligibility: Higher Ed ([accreditation](#)) and Sponsored Partners
2. [Agreement](#): InCommon Participation Agreement:
3. Delegating trusted Executive
4. Signed by an authorized representative
5. Pay Fees (\$700 registration & \$1,000 annual)
6. I.D. Proofing of Executive, appointment of Admin
7. Privacy/Security Policies/ posted ([Participant Operational Practices](#))

Technical Process

- Official Organizational Directory (IdM system)
 - Web Single Sign On (SSO)
1. Common Language: [eduPerson](#) schema
 2. Federating Software
 3. Federation I.D. Proofing of Admin
 4. Submit Metadata, Certificate Signing Request, and POP URL
 5. Install Certificate
 6. Test with Partners and Attribute Release Policies
 7. Deploy

InCommon Identity Assurance

- ▶ InCommon has finalized two documents that specify the criteria used to assess identity providers:
 - “Identity Assurance Assessment Framework”
 - “InCommon Bronze and Silver Identity Assurance Profiles”
- ▶ Supporting documents
 - InCommon Attribute Overview
 - InCommon Attribute Summary
 - Assurance Profile Assessment Checklist [EXCEL] — Should be used in conjunction with the InCommon "Identity Assurance Assessment Framework" and the InCommon "Bronze and Silver Identity Assurance Profile" documents. Is intended to aid in self assessment by IdP operators and provide background for a final assessment by qualified IT auditors.

Questions?

- ▶ Renee Shuey

- rshuey@psu.edu

- ▶ Resources

- <http://www.incommonfederation.org/>

- <http://www.incommonfederation.org/assurance/>

- <http://middleware.internet2.edu/eduperson/>

- <http://csrc.nist.gov/publications/PubsSPs.html>