Colorado Stat

Single Sign-On at Colorado State

Ron Splittgerber

Colorado State University
Colorado Stat

Agenda

- Identity Management
  - Authentication
  - Authorization
- The Problem
- The Solution: Federation
  - Trust Between Institutions
  - Trust Between Institution and Federal Portals
- Examples of Use

Identity Management

Who are you? (identification)

- Collect personally identifying information to prove you are who you say you are (identity proofing), such as drivers license, passport, or biometric data

- Assign attributes [(name, address, college or university, department, role (faculty, staff, student), major, email address]

How can you prove it? (authentication)

- Verifying that the person seeking access to a resource is the same one previously identified and approved

Identity Management

- Authentication does not verify that the person using the credential is who they say they are…
- It only establishes that the previously identified person is the same one who is seeking access to a resource.

Key Entities

Three entities involved in gaining access to a resource:

1.Subject (i.e. user) – The person identified and the subject of assertions (or claims) about his or her identity.

2.Identity Provider – Typically the university or organization that maintains the identity system, identity-proofs the subject and issues a credential. Also provides assertions or claims to the service provider about a subject's identity.

3.Service Provider (sometimes called the relying party) – Owner/provider of the protected resource to which the subject would like to access.

Key Terms

Authentication – Verification (via a user ID and password) that a subject is associated with an electronic identifier. This is the responsibility of the identity provider.

Authorization – Determining whether a subject is eligible to gain access to a resource or service. The authorization decision is made by the service provider and is based on the attributes provided by the identity provider.

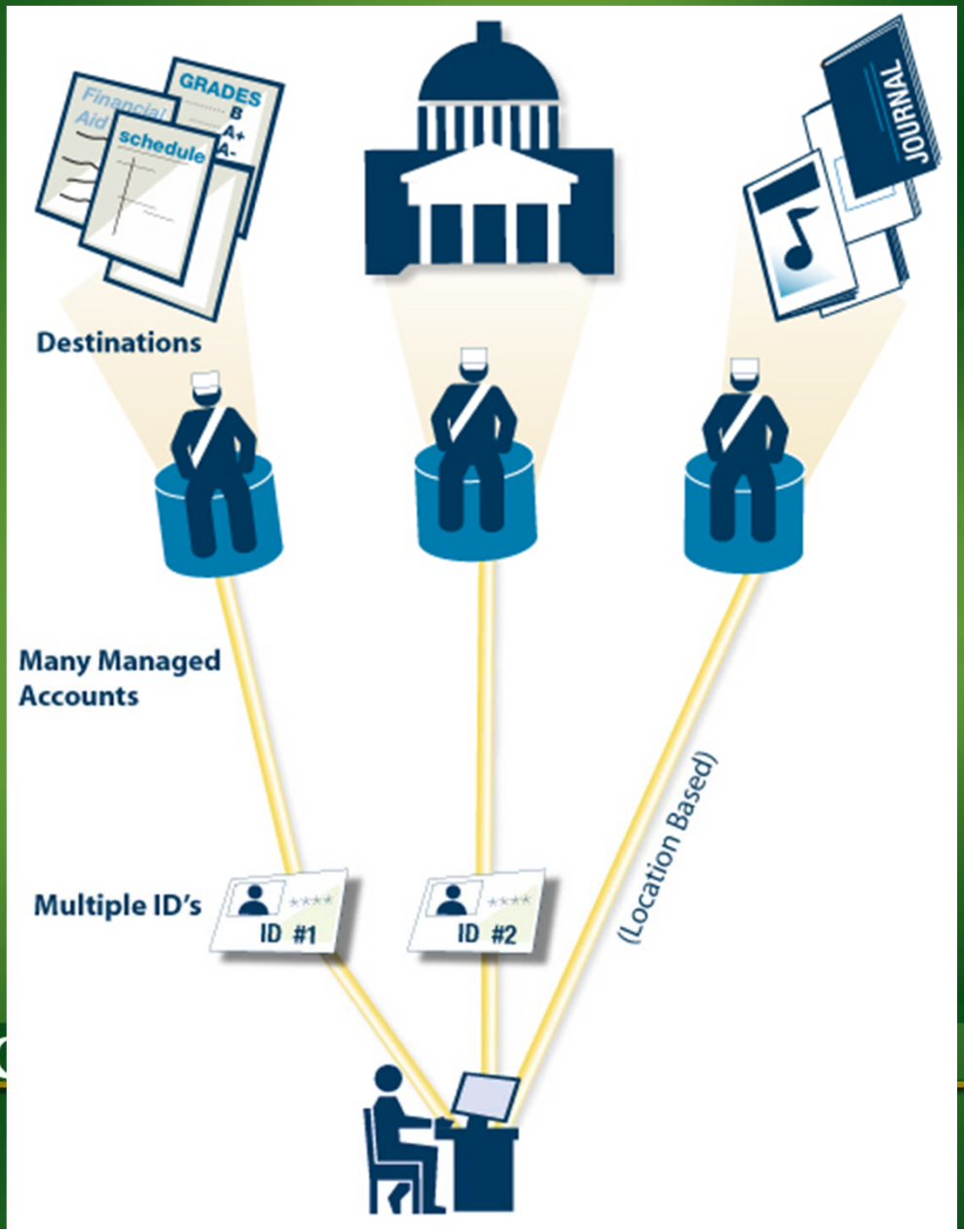
Attribute – Piece of information about an individual such as name, email address, role (faculty, staff, or student)

The Problem

- Growing number of applications – on-campus are outsourced or hosted
- All of these service providers must:
  - Verify the identity of users (faculty, staff, students, others)
  - Know who's eligible to access the service
  - Know the student is active and hasn't left school
- Increase in outsourced or external cloud services raises concerns about the security and privacy of the identity data

The Problem


What Do We Have InCommon?
Too Many Passwords...
Click here for more information > >



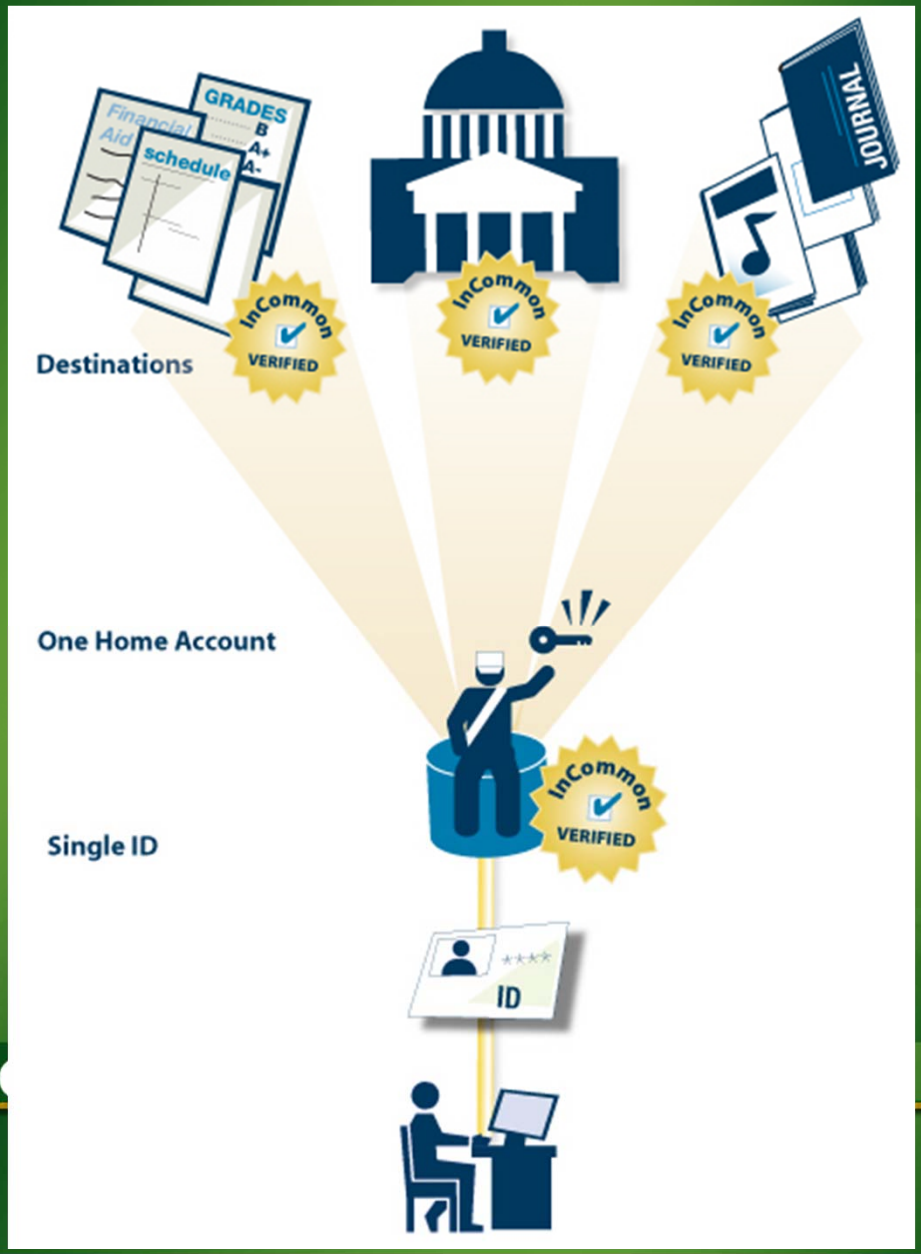
Without Federated ID

1. Users have many accounts to access needed resources
2. Access is based on user identity or location
3. Different login process at each resource
4. Many different passwords
5. Each resource provider must manage accounts / passwords
6. Lack of standards for password complexity, resets, format, etc.

A Solution: Federation of Identity

Federated identity management makes life easier for people who use web-based resources across institutions. It gives them access to multiple web sites that require login without requiring them to remember multiple IDs and passwords.

With federated identity management, institutions join together in a group, a federation, and agree to trust each other's identity credentials.



With Federated ID

- Users have single account to access the resources they need
- Access is based on trusted credentials from user' institution
- No overhead requirement for resource provider to manage accounts / passwords
- Private Information from user institution can be passed to resource as needed rather than having resource store it

InCommon Federation

InCommon is the federation for U.S. research and education, providing higher education and their commercial and non-profit partners with a common trust framework for access to online resources.

About InCommon

- Through InCommon, campuses leverage their identity databases to allow for the use of one set of credentials to access multiple resources.
- Online service providers no longer need to maintain user accounts.
- Identity providers manage the levels of their users' privacy and information exchange.
- InCommon uses SAML-based authentication and authorization systems (such as Shibboleth®) to enable scalable, trusted collaborations among its community of participants.

Advantages of Federated ID

- Convenience – Single sign-on with higher education credentials
- Safety – Enhanced security with fewer data spills
- Privacy – Release of only the minimum information necessary to gain access to resources (via attributes)
- Scalability – Once implemented, federated access relatively simple to extend
- Authentication – Campus does the authentication, maintaining control of user information
- Authorization – Service provider makes access decisions based on attributes

Federated Access in 30 seconds

4. If attributes are acceptable to resource policy, access is granted!

3. Authorization: Privacy-preserving exchange of agreed upon attributes

2. Federation-based trust exchange to verify partners and locations

1. Authentication: single-sign-on at home institution

Online Resource

Attributes: Anonymous ID, Staff, Student, …

Metadata, certificates, common attributes & meaning, federation registration authority, Shibboleth

Home Institution – user signs in

Colorado State University

Current InCommon Participants

Below is a complete list of InCommon Participants. There are also lists available for:

- Identity and Service Providers deployed in the federation (and other metadata-driven pages)
- Certificate Service subscribers

The IdP and SP pages include links to more-detailed information on each entity—just go to the IdP or SP list and click on the name of the IdP or SP you are interested in. **InCommon serves almost 6 million end-users through federated identity management.**

Higher Education Participants (282)	Government and Nonprofit Laboratories, Research Centers, and Agencies (22)	Sponsored Partners (106)
A. T. Still University	Ames Laboratory	Accessible Information Management, LLC
American University	Argonne National Laboratory	ALEKS Corporation
Amherst College	Brookhaven National Laboratory	Alexander Street Press
Arizona State University	ESnet	American Psychological Association
Arkansas State University	Fermilab	Apple - iTunes U
Augsburg College	GENI Project Office	ARTstor
Ball State University	Idaho National Laboratory	AT&T Services
Bay De Noc Community College	Internet2	Atlas Systems, Inc.
Baylor College of Medicine	Lawrence Berkeley National Laboratory	Atomic Learning
Baylor University	LIGO Scientific Collaboration	Benelogic
Beaufort County Community College	LTERN (Long Term Ecological Research Network)	BioOne, Inc.
Bloomburg University of Pennsylvania	Moss Landing Marine Laboratories	BioRAFT
Boise State University		Blackboard, Inc.
Boston University		Blatant Media Corporation

Federated Resources

Resources available via InCommon are many and diverse

Business Functions

- Benefits
- Asset management
- Talent management
- Visas & INS compliance
- Mobile alerts
- Travel management
- Energy management
- Surveys and market analysis

Learning and Research

- Journals
- Databases and analytical tools
- Multi-media access
- Homework labs
- Quiz tools
- Plagiarism detection
- Software downloading
- Alcohol awareness education
- Student travel discounts
- Transportation and ride-share services.

Colorado State University Colorado Stat

Strong support from key higher education partners, such as: Microsoft, Apple, National Student Clearinghouse, NSF, NIH, Gov-affiliated Labs

Single Sign-On

Single sign-on (SSO) is a session/user authentication process that permits a user to enter a user name and password one time in order to access multiple applications.

SSO is persistent – Allows session/user to access multiple applications by clicking on ‘Favorites’ link without having to re-enter user name and password

Single Sign-On with Federated ID

Why is this important?

- Username & Password from home institution
- More frequent password reset requirements
- Longer (15 characters or more) passwords
- Focus on collaborative research
- Increase in # portals for researchers
- Overhead of forgotten password changes
- Ability to transparently pass attributes

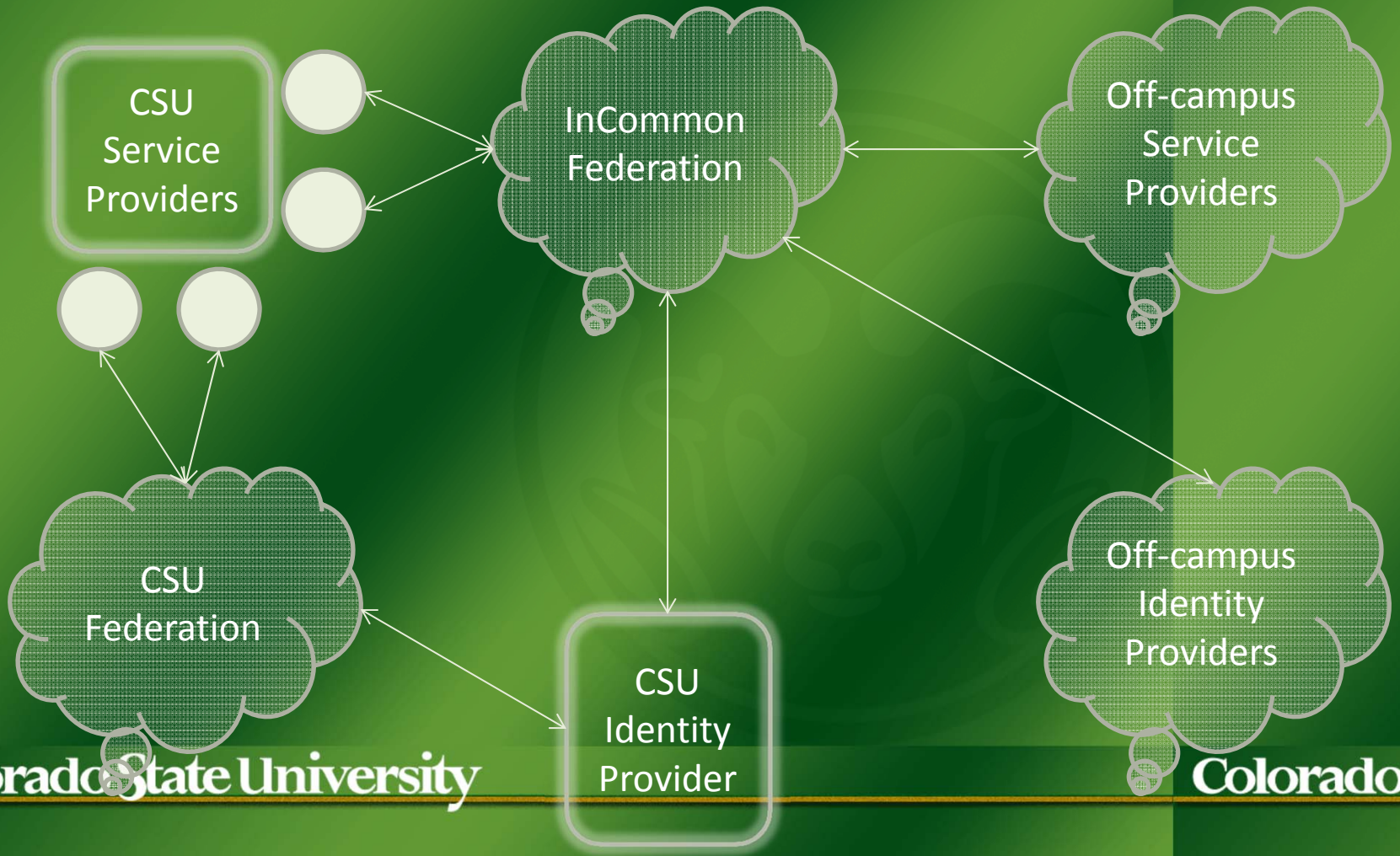
eduPerson Attributes

Can be passed to Portal to fill in forms, link profiles etc.

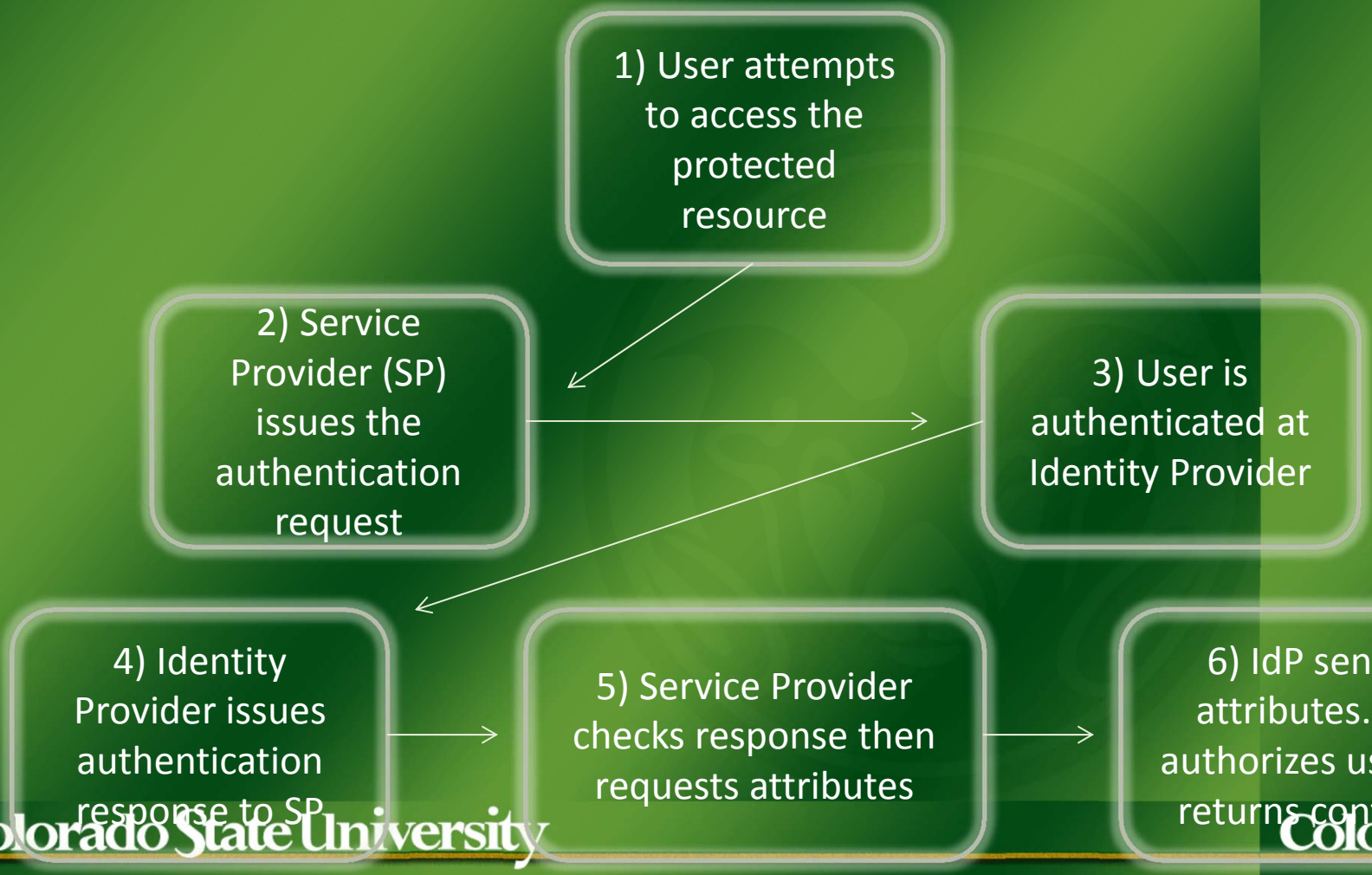
- eduPersonAffiliation
- eduPersonNickname
- eduPersonOrgDN
- eduPersonOrgUnitDN
- eduPersonPrimaryAffiliation
- eduPersonPrincipalName
- eduPersonEntitlement
- eduPersonPrimaryOrgUnitDN
- eduPersonScopedAffiliation
- eduPersonTargetedID
- eduPersonAssurance

The Federation Metadata Dance

Digitally signed Federation request is transferred over SSL



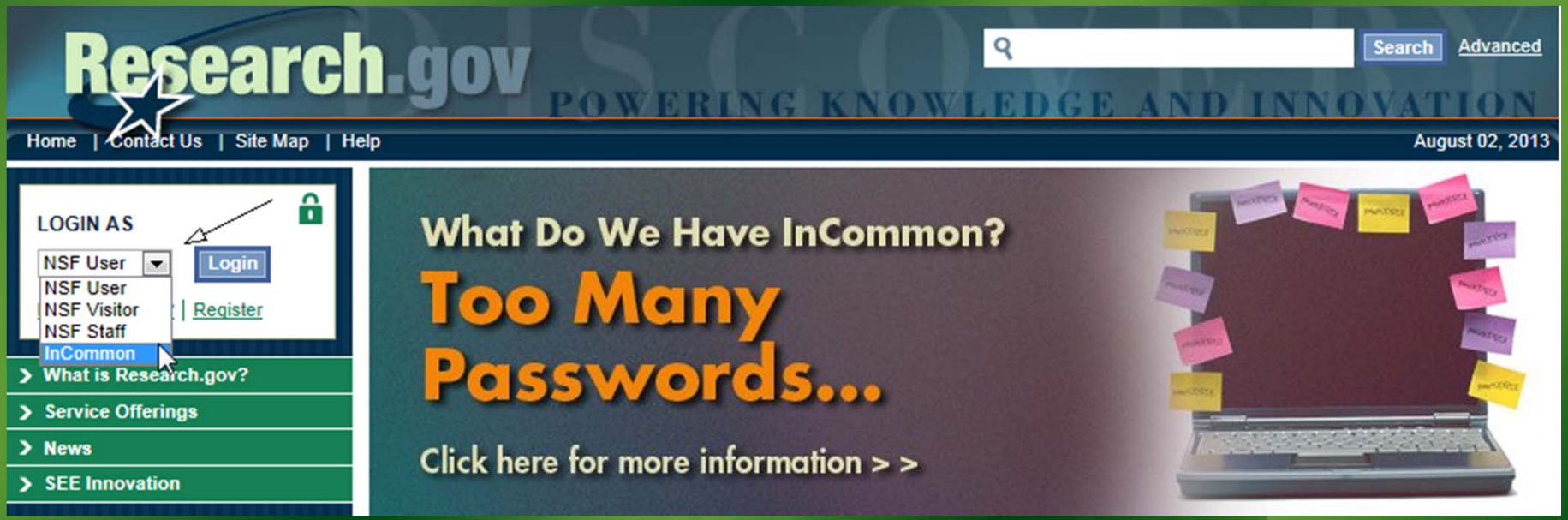
A Shibboleth Transaction



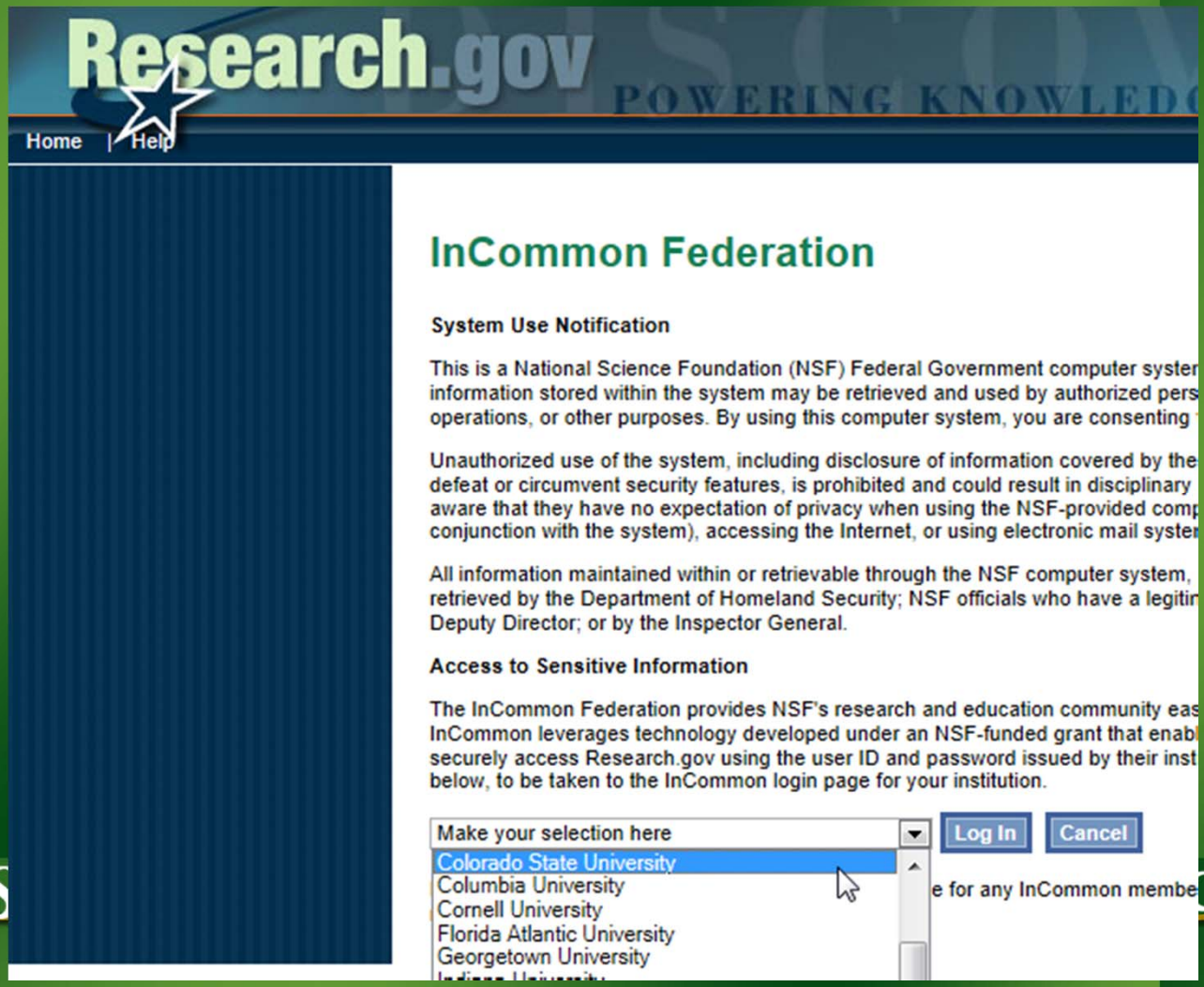
Examples of Use

- Research.gov
- NIH
- CSU Credentials
- Is My University Supported?

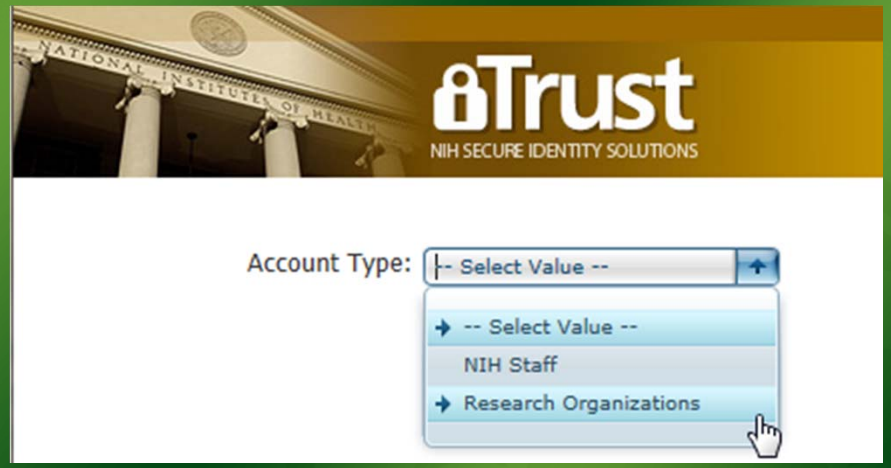
Research.gov

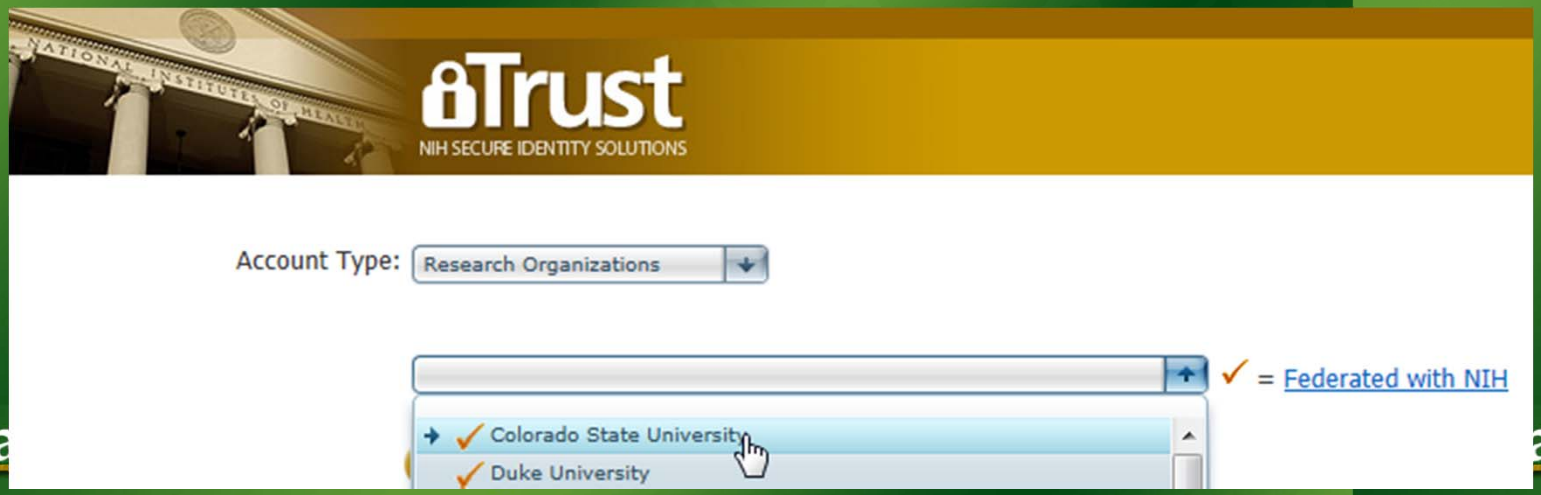


Research.gov

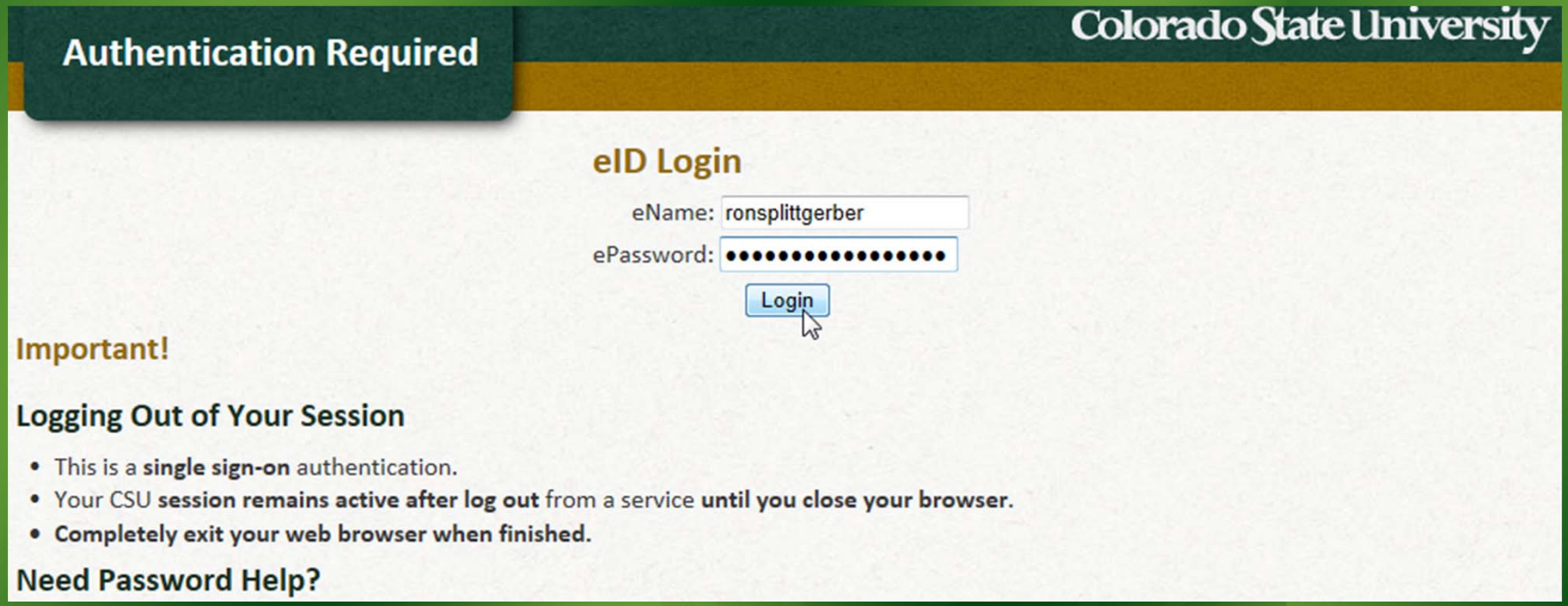


NIH Portals


eTrust
NIH SECURE IDENTITY SOLUTIONS
Account Type:
-- Select Value --
-- Select Value --
NIH Staff
Research Organizations


eTrust
NIH SECURE IDENTITY SOLUTIONS
Account Type:
Research Organizations
= Federated with NIH
Colorado State University
Duke University

My Local Identity Provider




Research.gov
POWERING KNOWLEDGE AND INNOVATION
Search
Advanced
Home | Contact Us | Site Map | Help
Welcome Ronald Splittgerber | My Profile | Logout | August 02, 2013
MY DESKTOP
Research.gov Services & Tools
Research Spending & Results
Policy Library
What is Research.gov?
Service Offerings
News
SEE Innovation
What Do We Have InCommon?
Too Many Passwords...
Click here for more information > >

Colorado Stat

Is My University Supported?

Higher Education Participants (378)

A. T. Still University
Allegheny College
American University
Amherst College
Arizona State University
Arkansas State University
Auburn University
Augsburg College
Azusa Pacific University

Colorado State Univers
Colorado Stat

Questions?