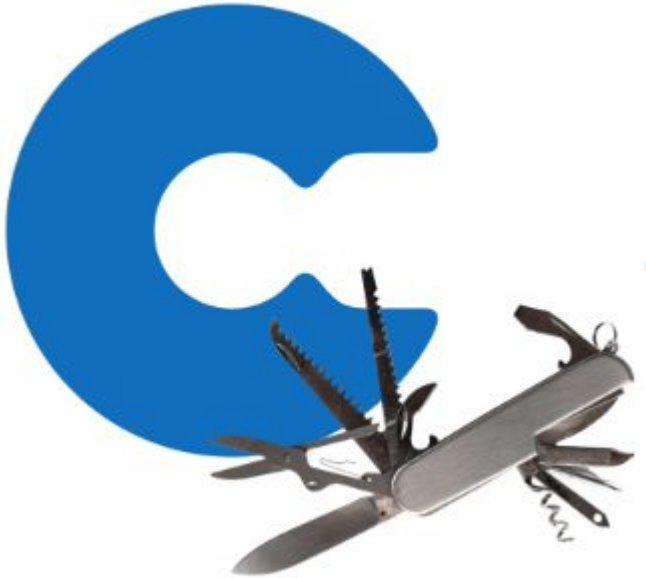
cirrus identity

FIM4R Talk
Providing Solutions to Collaborations



©Cirrus Identity, Inc.

Ask:

Given your experience in working with and supplying solutions to all kinds of collaborations, would you be willing to give a presentation on status and challenges you see that especially smaller collaborations face ?

©Cirrus Identity, Inc.

- Cirrus Identity Experience in the field over the past decade +
- InCommon Federation Proxies Working Group (which leveraged the AARC blueprint as reference)

©Cirrus Identity, Inc.

Different kinds of proxies

- Infrastructure
- “Community”

There are many different types and sizes of communities with very different audiences and needs

- Level of assurance
- Attribute persistence and manipulation
- User experience
- And more

©Cirrus Identity, Inc.

Brief Background of Cirrus Identity's experience in the field

©Cirrus Identity, Inc.

Cirrus Identity is probably most known for the Cirrus Bridge

Connect commercial IdPs to multilateral trust frameworks

©Cirrus Identity, Inc.

Cirrus Identity Enterprise Bridge

Service Providers / Applications

Multilateral federated SAML Applications

Multilateral SAML Authentication

SAML Bridge

Identity Provider

Microsoft Entra ID

Cirrus Identity first launched with a very simple goal

Help application developers integrate social login with campus applications

Classic infrastructure proxy -
Protocol translation, attribute mapping

©Cirrus Identity, Inc.

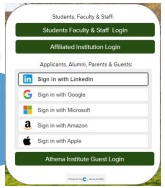
Cirrus Identity - The beginning

Service Providers

Application

Cirrus Gateway

Cirrus Discovery



External IdPs

Identity Providers

©Cirrus Identity, Inc.

Campus Community Use Cases

Alumni access
Continuing and Professional Education
Parent Access

©Cirrus Identity, Inc.

Campus Community - Common Campus Use Case with Social Login

Service Providers

Application

Application

Application

Institution's User Data (IDMS)

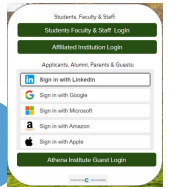
API

Cirrus Account Linking

ID Verify Add-On

Cirrus Authentication Proxy

Cirrus Discovery



Cirrus Gateway

Identity Providers

Institution's Identity Provider

Cirrus OrgBrandedID

External IdPs

Campus Community Research Use Cases

- Campus App with External Partners - eAdmin for research
- Campus/medical center collaboration
- Grant-funded research at a campus - desire to leverage multilateral federation

©Cirrus Identity, Inc.

Cirrus Research Community - Initial Research Architecture

Service Providers

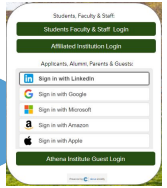
Application

Application

Application

Cirrus Authentication Proxy

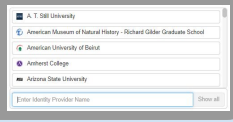
Cirrus Discovery

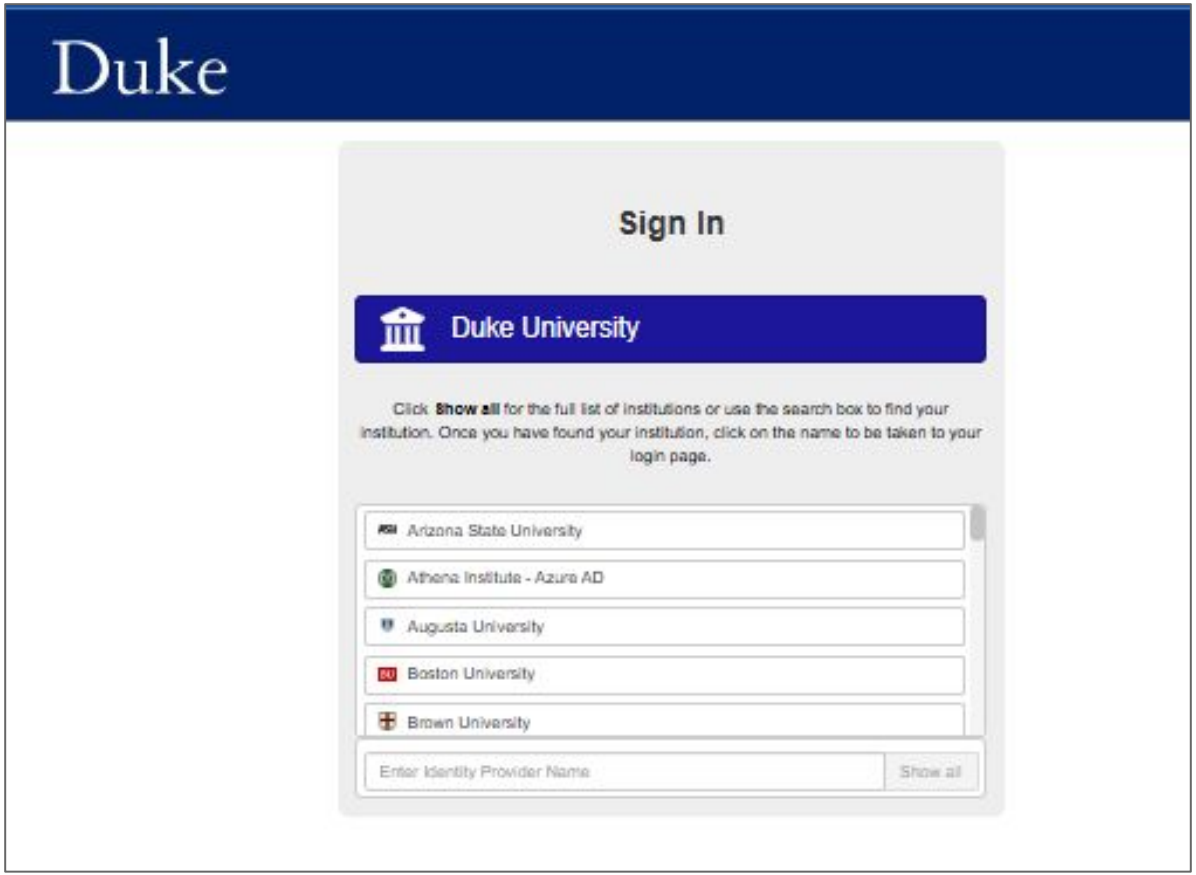


Identity Providers

Institution's Identity Provider

InCommon IdPs





©Cirrus Identity, Inc.

Campus Community Research Use Cases
Evolving Needs

- Need access for users with no trusted IdP (IdPoLR)
- Need integration with trusted partners who do not wish to join the federation (“Proxy connector”)
- Need for MFA signaling and enforcement

©Cirrus Identity, Inc.

Cirrus Identity - Evolving Research Architecture

Service Providers

Application

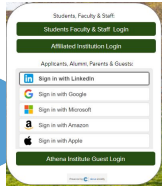
Application

Application

Cirrus MFA

Cirrus Authentication Proxy

Cirrus Discovery



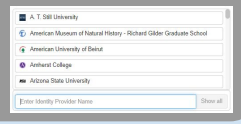
Proxy Connector

Identity Providers

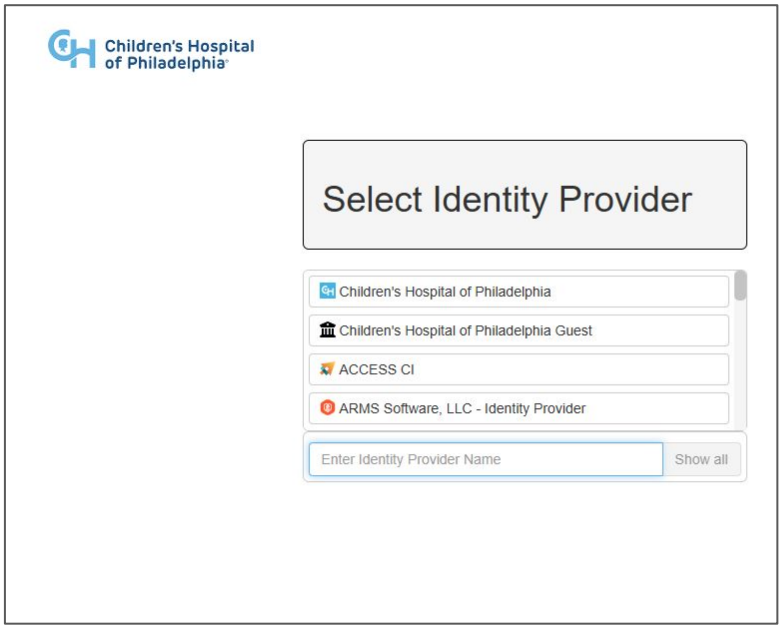
Institution's Identity Provider

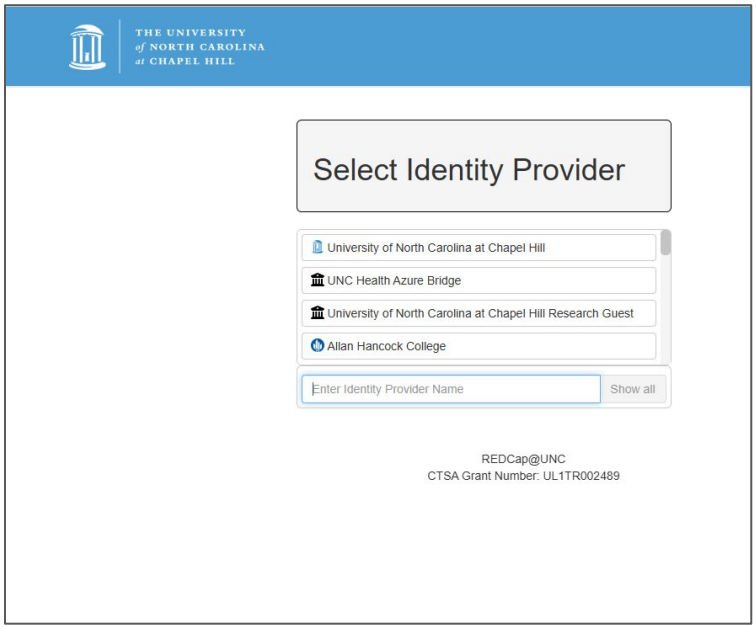
Institution's Affiliated Identity Provider
(Not InCommon)

InCommon IdPs



Cirrus OrgBrandedID





©Cirrus Identity, Inc.

Regional Collaboration Use Cases

- State system-wide service access
- Learning Management Systems (Canvas, D2L)
- ERP solutions (WorkDay)

©Cirrus Identity, Inc.

Cirrus Identity - Evolving Research Architecture

Service Providers

Application

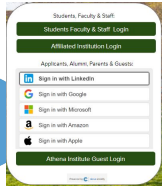
Application

Application

Cirrus MFA

Cirrus Authentication Proxy

Cirrus Discovery



Proxy Connector

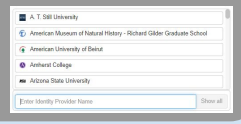
Cirrus Gateway

Identity Providers

Institution's Identity Provider

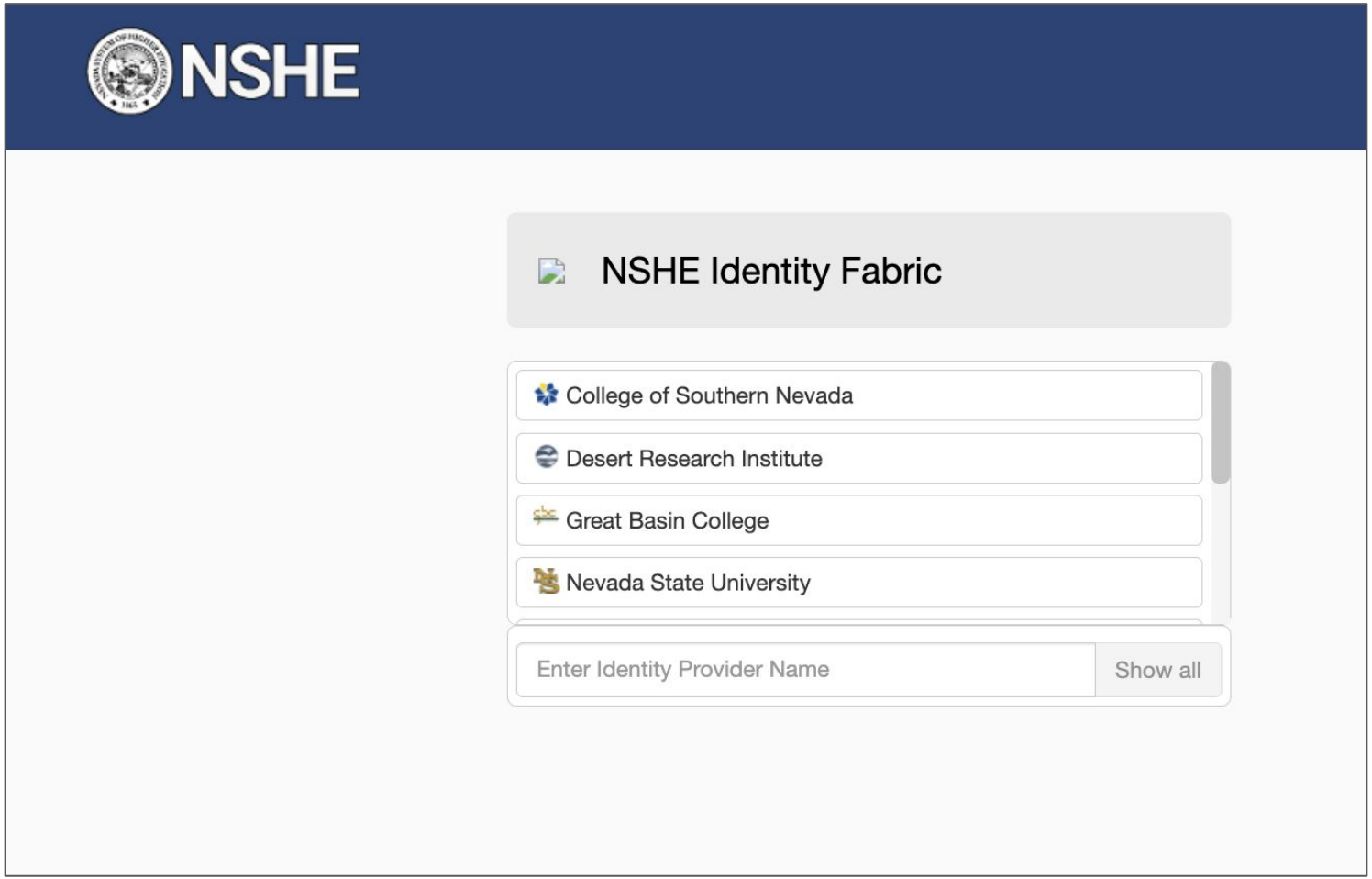
Institution's Affiliated Identity Provider
(Not InCommon)

InCommon IdPs



Cirrus OrgBrandedID

External IdPs



©Cirrus Identity, Inc.

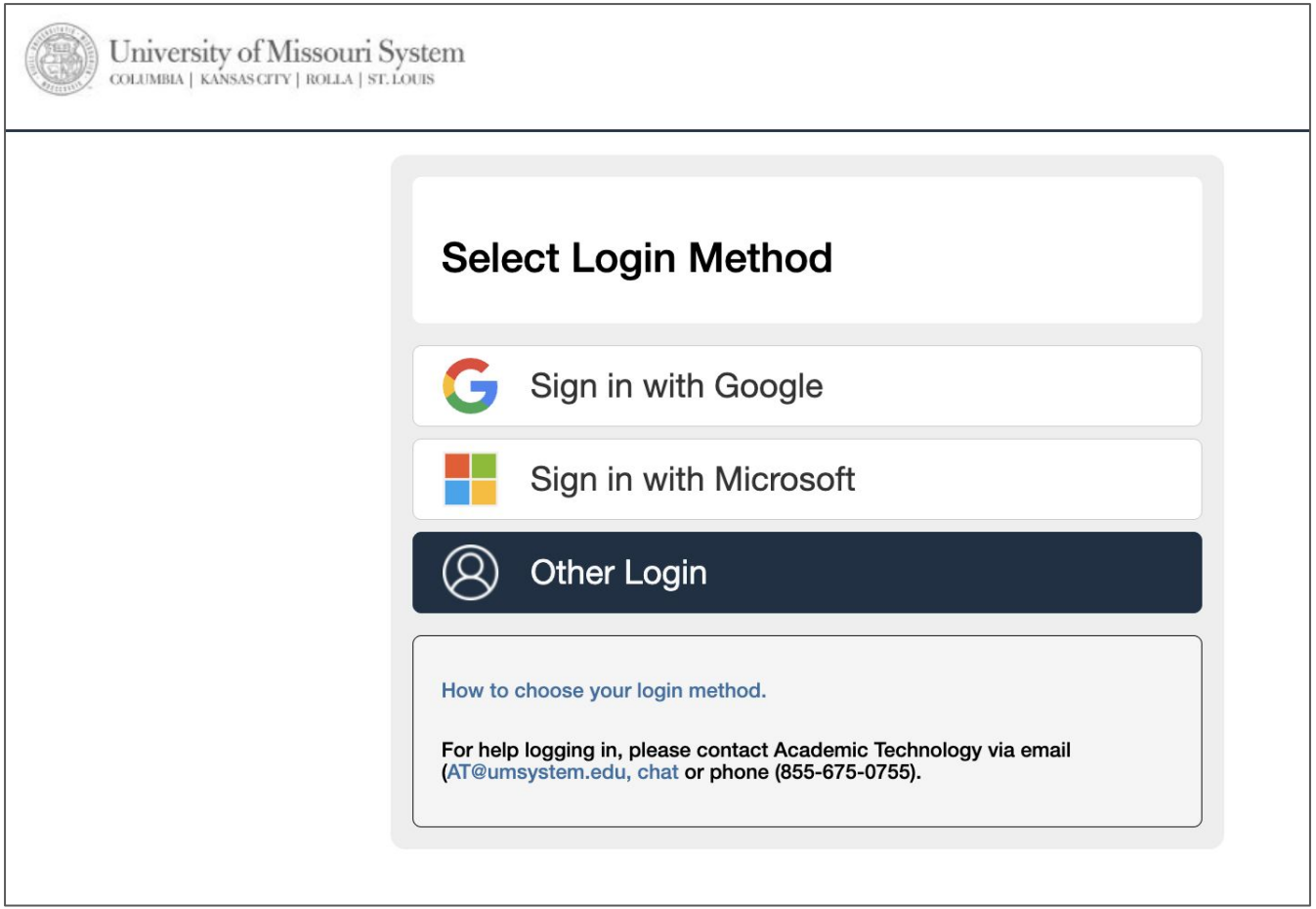
University of Missouri System
COLUMBIA | KANSAS CITY | ROLLA | ST. LOUIS

UMSYSTEM
LOGIN →
Use this log in with your UMSystem credentials.

ALTERNATIVE
LOGIN →
Use this log in if you do not have University credentials and have not received an invitation.

Get help choosing a log in method.

©Cirrus Identity, Inc.



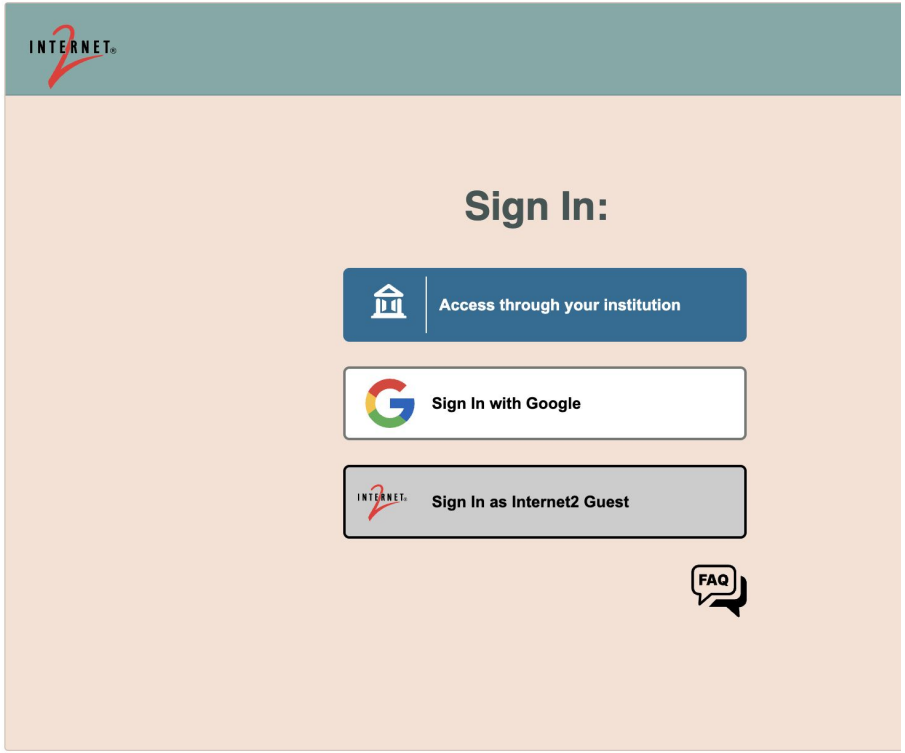
©Cirrus Identity, Inc.

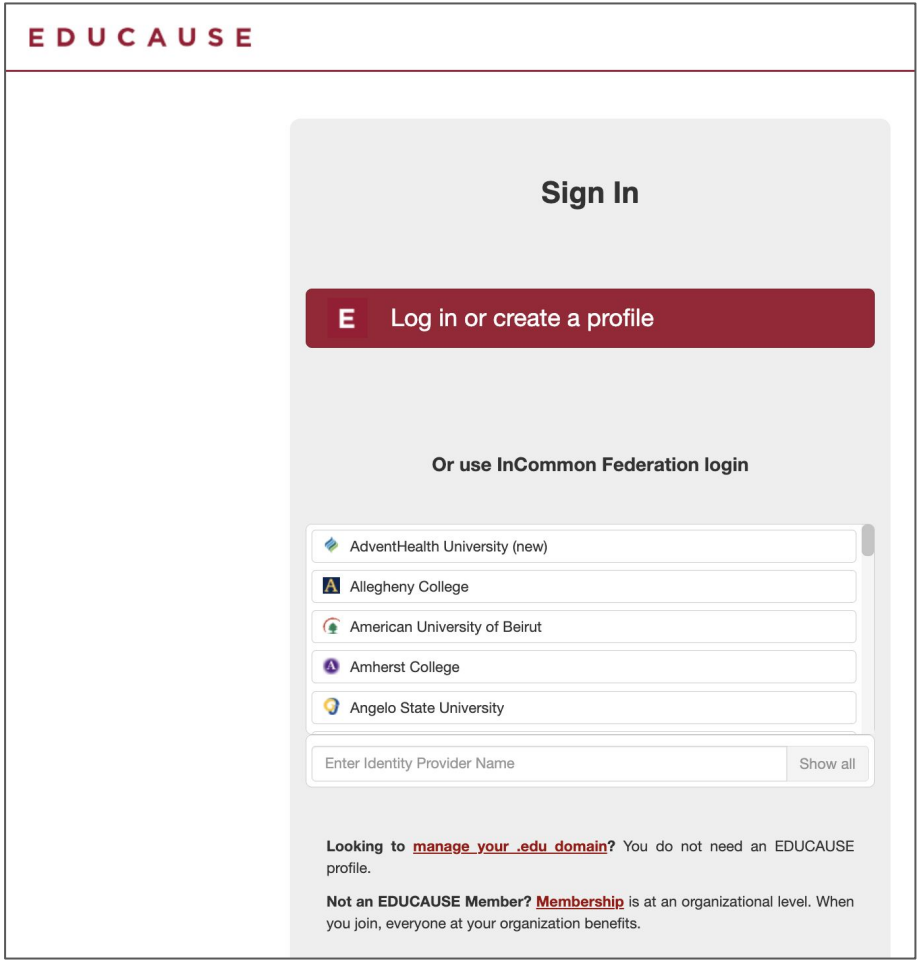
Larger Community Collaboration

- Internet 2
- EDUCAUSE
- National Science Foundation

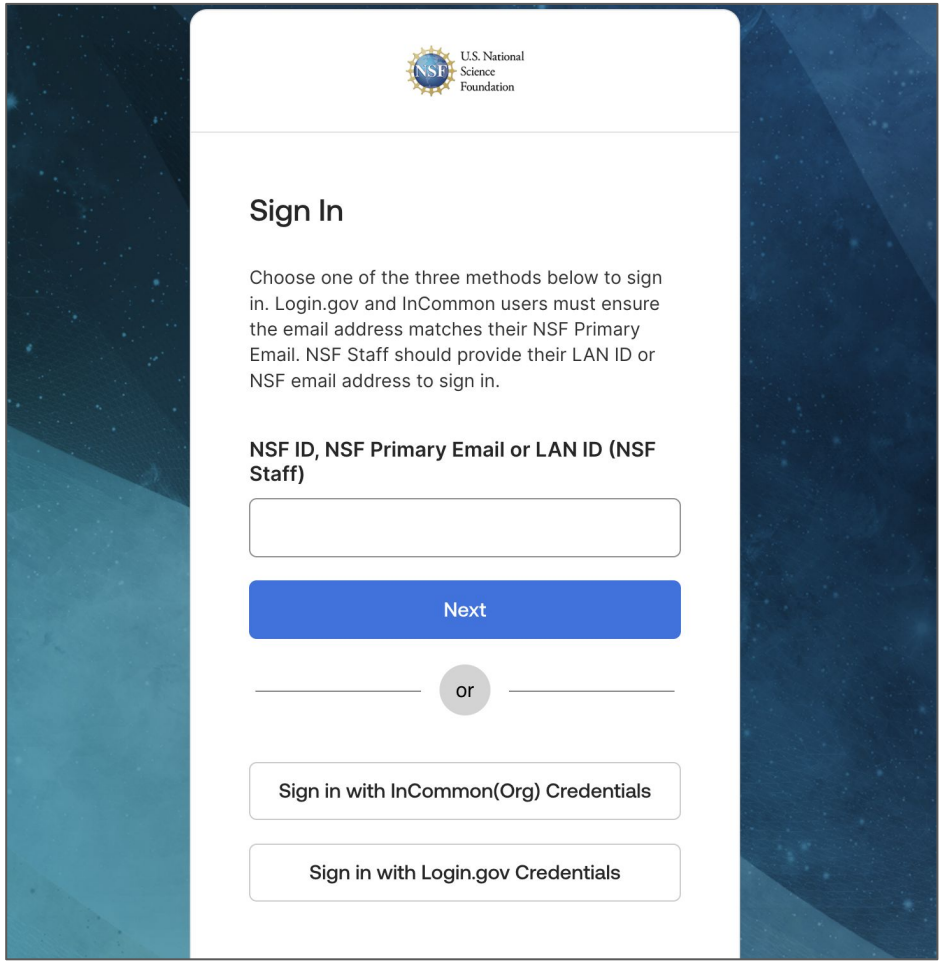
Various ways to onboard users and link identifiers used for authorization

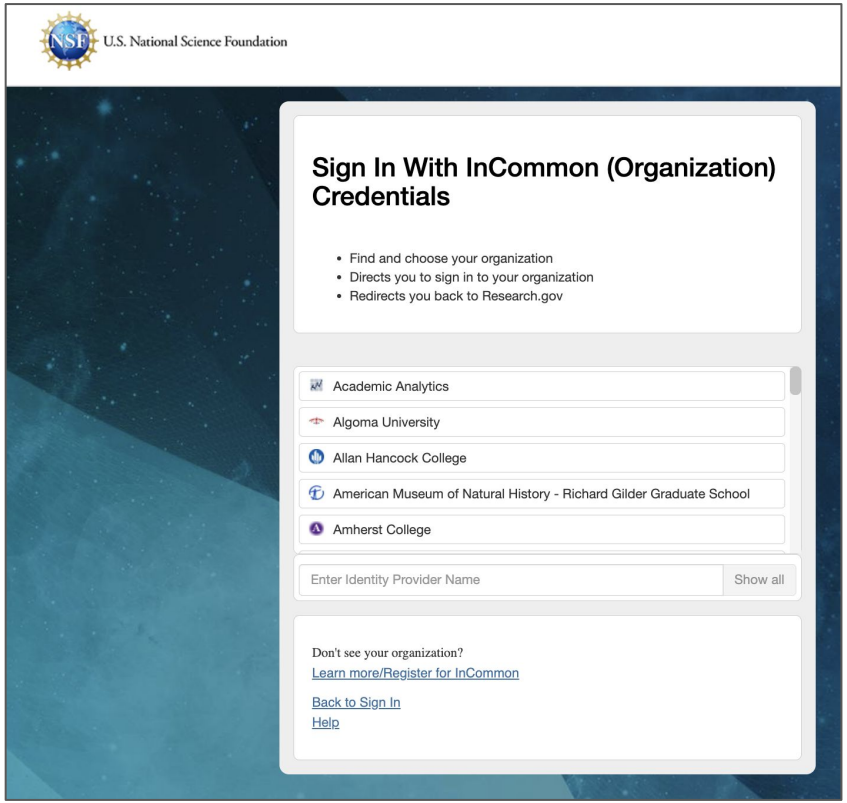
©Cirrus Identity, Inc.





©Cirrus Identity, Inc.





©Cirrus Identity, Inc.

Cirrus Identity - High Level Research Architecture

Service Providers

Application

Application

Application

SAM, OIDC, CAS Authentication

Cirrus MFA

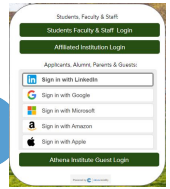
Institution's User Data (IDMS)

API

Cirrus Account Linking

Cirrus Authentication Proxy

Cirrus Discovery



Cirrus Gateway

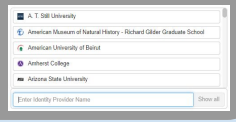
Proxy Connector

Identity Providers

Institution's Identity Provider

Institution's Affiliated Identity Provider (Not InCommon)

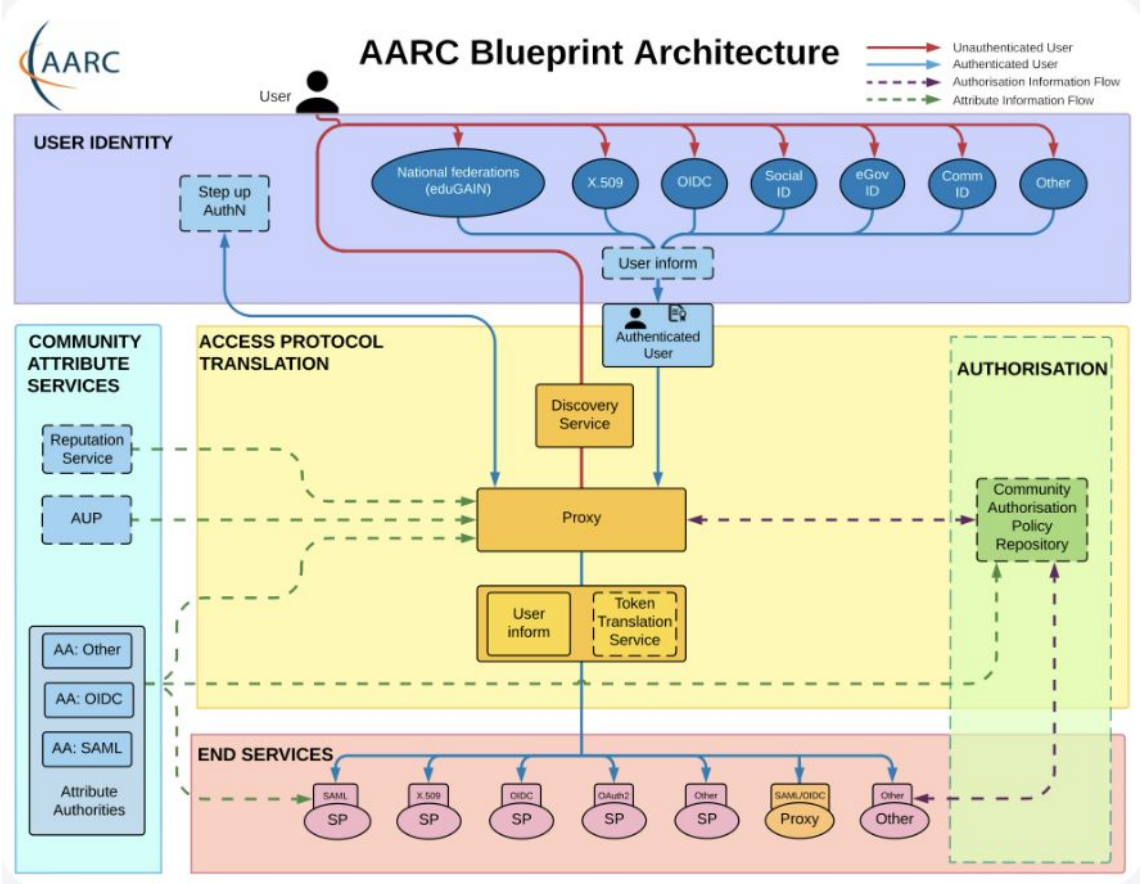
InCommon IdPs



Cirrus OrgBrandedID

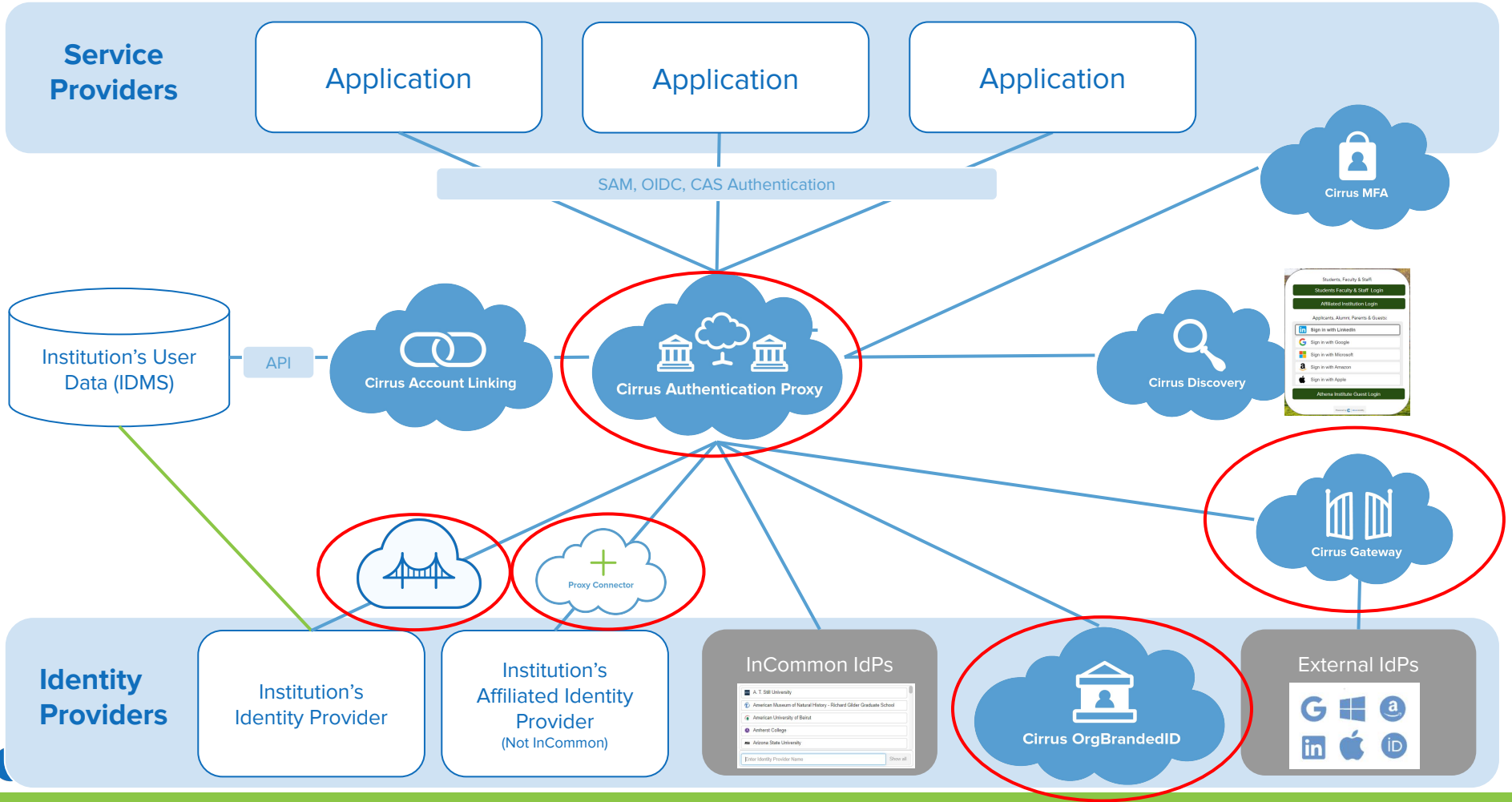
External IdPs

©Cirrus Identity, Inc.



©Cirrus Identity, Inc.

Cirrus Identity - High Level Research Architecture



Primary Lesson Learned

Design the Solution to
Fit the Needs of the Community

©Cirrus Identity, Inc.

Key Principles We Follow

©Cirrus Identity, Inc.

Respect, promote, and honor the core principles and values of multilateral trust federation as much as possible

- Educate functional and technical stakeholders about the value of multilateral federation
- Be a part of the community - work closely with federation operators and members

©Cirrus Identity, Inc.

Support key REFEDS specifications as they evolve

- MFA signaling
- R&S attributes (and other attribute specifications as developed)
- Level of Assurance frameworks as they evolve

Participate in workgroups that develop and update standards

©Cirrus Identity, Inc.

Incentivize participation in the federation

- Provide cost disincentives to non-federation participation
- But also provide options for hybrid collaborations - do offer options that enable collaboration for non-federation participants. This is better than long-term pressure to
  - leverage commercial solutions for trust
  - create duplicate/overlapping federations
- Create a pathway for federation onboarding

©Cirrus Identity, Inc.

Establish attribute requirements and expectations up front

- What attributes will the SPs require?
- Do all the IdPs participating assert those attributes?
- Are there any specific authorization requirements for SPs that IdPs need to support?
- Is there an existing registry of users with unique IDs? Will there need to be one?

©Cirrus Identity, Inc.

Persist, manipulate, or otherwise transform data as little as possible

- Acting as a simple broker is best where possible
- The less data you persist, the fewer the compliance requirements and more intuitive the integration
- Where data is persisted and/or manipulated - maintain full transparency and have strong data management practices

©Cirrus Identity, Inc.

Leverage Multi-Proxy deployments for different audiences

- Even within the same organization, different stakeholders will have different needs and interests around
  - User on-boarding experience
  - IdPs they wish to allow
  - Login/discovery experience

Better to encourage use of common attribute collections, but support deployment of more than one proxy for different audiences

©Cirrus Identity, Inc.

Questions/thoughts

©Cirrus Identity, Inc.