



**cirrus** identity

# Cirrus Bridge Webinar

**Learn about the Cirrus Bridge and Multilateral Federation!**

Hear directly from Cirrus customers on how they simplified their SAML & CAS IAM environments with the Bridge cloud solutions

**Your Swiss Army Knife of Simple and Secure Login Solutions**

**for higher education and enterprise**

<https://www.cirrusidentity.com>

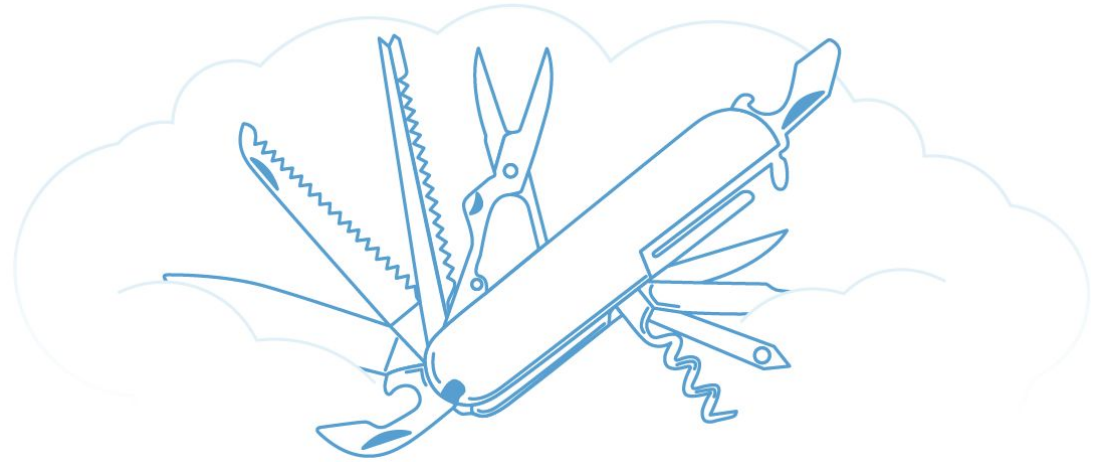
# Welcome & Introduction!

**By Dedra Chamberlin**

Cirrus Identity CEO & Founder

# Who is Cirrus Identity?

Your Swiss Army Knife for  
Digital Identity Management



# Focus for Today's Webinar



## Cirrus Bridge

Upcoming Webinars in Our Series:  
Social and OrgBrandedID Login for  
Alumni and Online Learning



# Webinar Goals

1. Share higher ed trends and why institutions are moving to the Cirrus Bridge solutions
2. Explain more about multilateral federation and the gaps in commercial products
3. Hear about “real” implementations from Cirrus Bridge customers

# Agenda & Introductions

1. **Cirrus Bridge Institutional Drivers & Key Features - Mark Rank, Cirrus Director of Product, Cirrus Identity - 10 min**
2. **Multilateral Federation and Gaps with Commercial SSO Solutions - Patrick Radtke, Cirrus Chief Technology Officer, Cirrus Identity - 10 min**
3. **Cirrus Bridge Customer Panel - 20 min**
  - a. **Kevin Hickey, Director of Information Security, University of Detroit Mercy**
  - b. **Molly McDermott, Sr. Project Manager, Illinois Institute of Technology**
  - c. **Mike Dulay, Director of Web Tech Services, Millersville University**
4. **Open Forum Questions & Answers - 15 min**

# Cirrus Bridge: Institutional Drivers for Higher Ed & Key Features

**By Mark Rank**

Cirrus Identity Director of Product

## Some of the things Cirrus hears:

- Our organization has three different single sign-on services, why can't we have ONE?
- Research staff keep asking for this thing called "InCommon"
- Researcher's with NIH grants say they need MFA to keep accessing grant services

**Drivers:**

**User Experience!**





**Drivers:**  
**Organizational  
Resources!**

## Some of the things Cirrus hears:

- We have an executive that keeps asking “Why are we running this, isn’t there a cloud solution?”
- The person that ran Shibboleth/Apereio CAS just retired, no one else wants to take it over
- There are no staff to run access management services
- We get Azure AD with our O365 subscription, “Why can’t we use that for everything?”



## Drivers: Technical Consolidation!

### Some of the things Cirrus hears:

- We have on-prem AD with ADFS and we want to move to a cloud SSO solution for better availability
- We are moving to <insert commercial SSO provider>, but we have 50/100/500/”I Don’t Know” service providers integrated with Shibboleth/Apereo CAS
- We are moving to <insert commercial SSO provider>, but we have a bunch of apps that only integrate with the CAS protocol
- We moved to <insert commercial SSO provider> and access to our Research/Library/Learning apps broke
- We are implementing MFA using Microsoft/Okta - everything needs to authenticate there



# IdPaaS Working Group

## InCommon Federation Identity Provider as a Service Working Group Final Report

**Repository ID:** TI.145.1  
**Persistent URL:** <http://doi.org/10.26869/TI.145.1>  
**Document Status:** Submitted  
**Publication Date:** December 4, 2020  
**Sponsor:** InCommon Technical Advisory Committee

### Executive Summary

The [Identity Provider as a Service Working Group](http://doi.org/10.26869/TI.145.1) was chartered by the InCommon Technical Advisory Committee (TAC) in March 2019 to analyze community needs and recommend how InCommon can make Federation participation more accessible through support of cloud-based Identity Provider as a Service (IdPaaS) solutions.

<https://spaces.at.internet2.edu/display/TI/TI.145.1>



Cirrus Bridge

## What is it?

- The IdPaaS report defined a “**Federation Adaptor**” as “A service that operates as a bridge between Federation and Intracampus single sign-on(SSO)” - this is the base integration model covered by the report
- The need for a federation adaptor is widely seen by Cirrus Identity, and the Cirrus Bridge meets that need.
- Technically, it is an optimized authentication proxy implemented using the widely adopted simpleSAMLphp framework (<https://simplesamlphp.org/>) and offered to customers as a managed service
- In addition to federation enablement, the Cirrus Bridge also incorporates other key features



## Key Features of the Cirrus Bridge


SAML Bridge	CAS Bridge	Also!
<ul style="list-style-type: none"> <li>• Supports multi-lateral federation required by InCommon and other eduGAIN federations.</li> <li>• Supports REFEDS Research and Scholarship standard release of attributes.</li> <li>• Supports REFEDS multi-factor authentication (MFA) context to meet the MFA signalling requirements.</li> <li>• No need to maintain local SAML IdP (Shibboleth/SSP/ADFS)</li> </ul>	<ul style="list-style-type: none"> <li>• Authentication support for CAS service providers from a SAML IdP</li> <li>• Transformation of SAML assertions into CAS tickets</li> <li>• Modern CAS implementation with security protections against replay attacks</li> <li>• No need to maintain local CAS IdP (Shibboleth/Apereo CAS/SSP)</li> </ul>	<ul style="list-style-type: none"> <li>• DNS Add-On available to quickly shift existing services to the Cirrus Bridge – allows for time to natively integrate services directly with a commercial SSO solution</li> <li>• Conditional Access supports the granular access control features available in Azure AD or Okta (such as attribute release, authorization by groups, MFA, encryption options, and visibility in “App Portals”) – allows configuration from the Azure or Okta admin portals</li> </ul>

# Federation Adapter in Pictures


Service Providers






CAS Services



Local or Cloud SAML



Multilateral SAML




CAS Authentication

SAML Authentication



CAS Bridge

DNS Add-On





SAML Bridge


DNS Add-On

Identity Providers

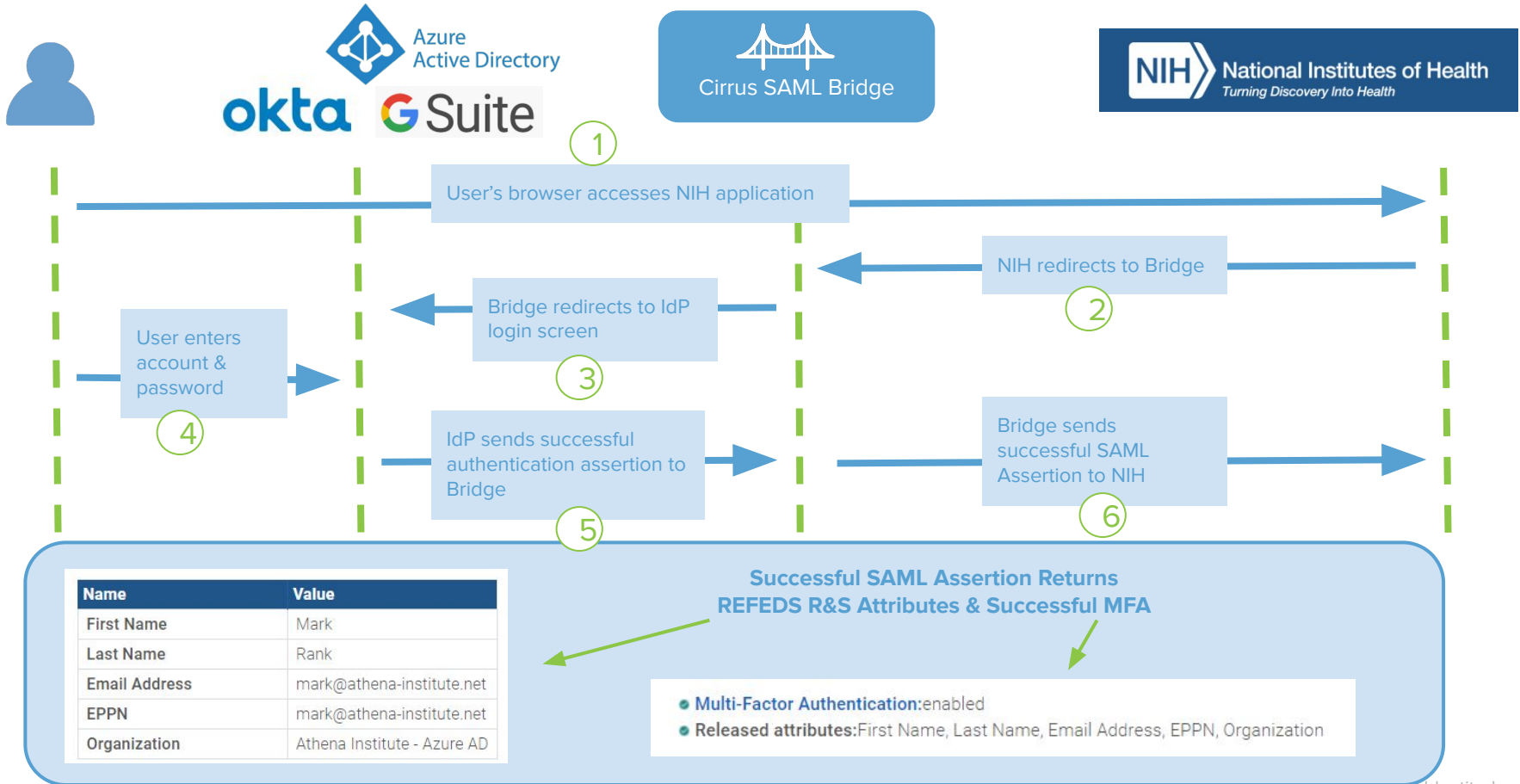
Institutional Identity Provider Options



Azure Active Directory



# High Level Authentication Flow - SAML Bridge



Cirrus Identity is a **Trusted** InCommon Catalyst Partner






# Multilateral Federation


**By Patrick Radtke**

Cirrus Identity CTO

- How can you scale trust?
- As cross university research team, do you want to spend time contacting universities individually to perform an integration with your research app?
- As an IdP operator, do you want to individually evaluate and configure integrations to the thousands of research applications?
- Could these tasks, and more, be handled by a trusted third party?



## Metadata Explorer Tool


Access through your institution

### Entities summary

ENTITIES	IDP	SP	AA
21055	7230	13818	7

Most Federated Entities
Search Entities

### Interfederations summary

NAME	ENTITIES	IDP	SP	AA
eduGAIN	8280	4771	3519	2

**Total:** 1
Export ▾

# What does the Multilateral Federation do?

- Scale relationships between multiple organizations (identity providers) and applications (service providers) around the world.
- Vet IdPs and SPs, and ensure conformance to baseline expectations.
- Gather and aggregate metadata (signing keys, login URLs, contact info, etc) about their identity providers and service providers
- Provide a framework for interoperability. Example: Research and Scholarship
- **End result:** a trust framework that allows a Service Provider to trust hundreds of Identity Providers at once (and vice-versa) without a time-consuming individual integration



Identity Providers



Service Providers

## For registration

- The Identity Provider (IdP) entityId is in your domain space.
- The IdP has one single sign on endpoint, where users are sent to authenticate.
- No more than 2 signing keys

## For interoperability

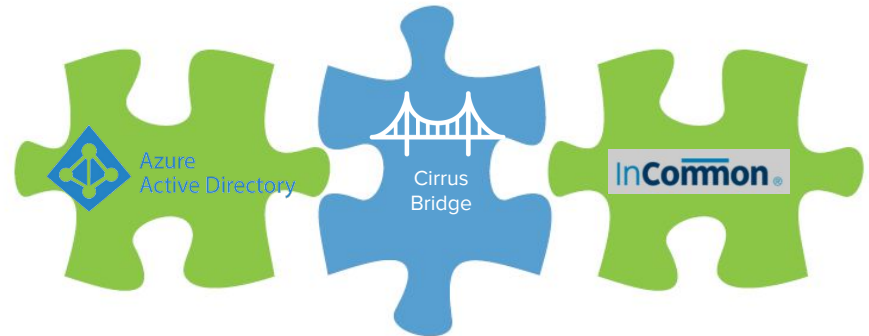
- IdP can query federation metadata to learn about new or changed service providers
- Can signal MFA using REFED's MFA Profile
- Keep up with new base line expectations

## For operational management

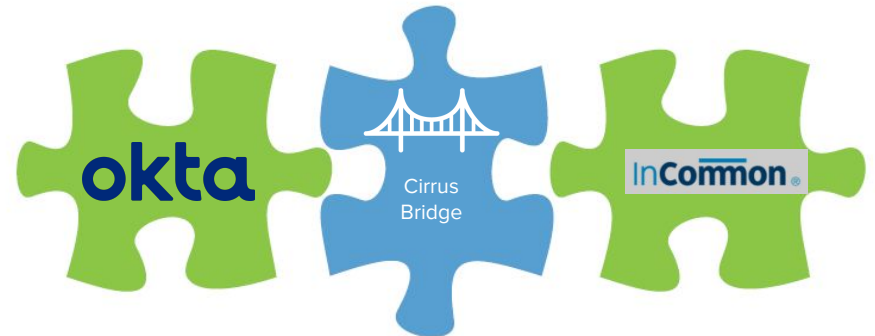
- Allow attribute release by entity category
- Allow attribute release by mechanism other than SP entityId

# Multilateral Federation Gaps with Azure AD

- IdP Entity ID is not under campus domain. It is under <https://sts.windows.net/>
- Azure AD does not query or consume multilateral federation metadata
- Signals Multifactor in way not compatible with REFEDS MFA.
- Azure AD does not support attribute release based on entity categories, such as REFEDS Research and Scholarship (R&S)
- Non-premium Azure AD subscription levels:
  - a. No control over SAML key rotation
  - b. Generates a SAML key per Azure application, can be 3 keys
  - c. No control over attribute naming

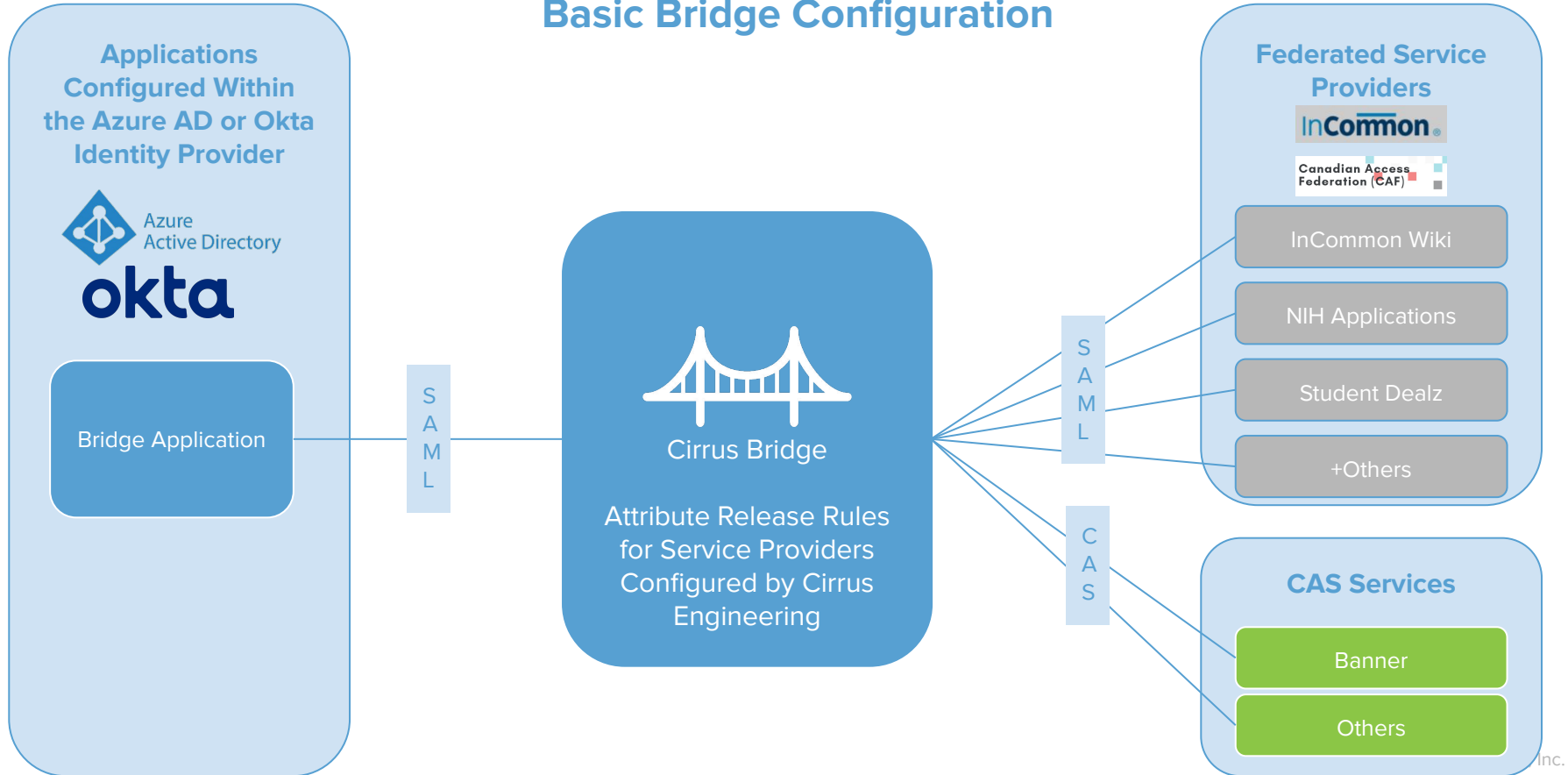


- Each Okta Service Provider integration creates a unique Single Sign On endpoint.
- Okta does not query or consume multilateral federation metadata
- Okta does not support rules based on attributes in the federation metadata, such as those required for the REFEDS Research and Scholarship (R&S)
- Signals Multifactor in way not compatible with REFEDS MFA.



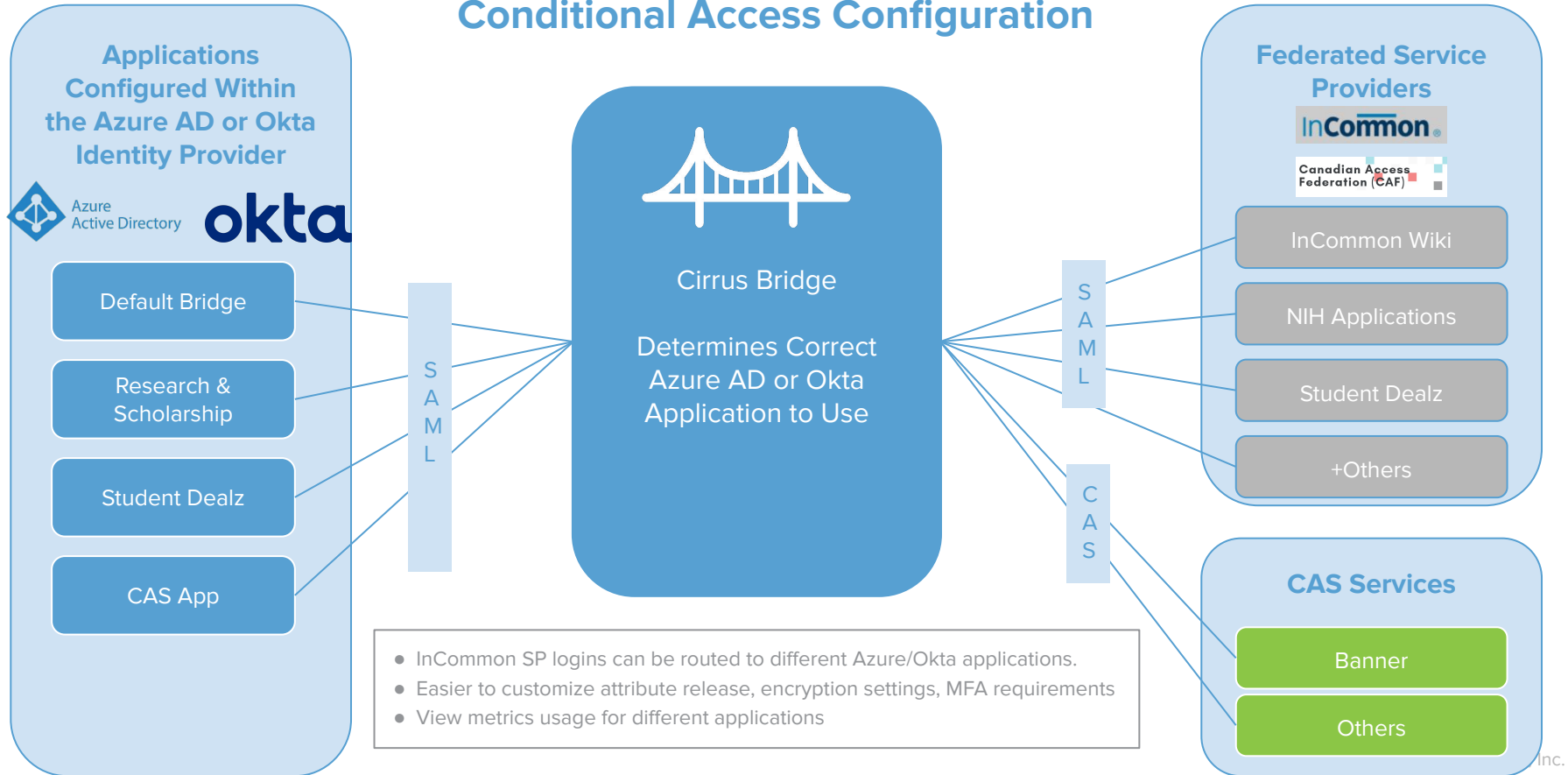
# How the Cirrus Bridge Solves Multilateral Federation

## Basic Bridge Configuration



# How the Cirrus Bridge Solves Multilateral Federation

## Conditional Access Configuration





## Cirrus Bridge Materials

- [Cirrus Bridge Website Link](#)
- [Identity Provider as a Service Work Group report](#) from InCommon Technical Advisory Committee
- [EDUCAUSE article - Cloud First Approach for NIH and Academic Research Access](#)
- [Cirrus Identity announces integration with Microsoft Azure Active Directory to help universities meet deadline for new NIH authentication requirements](#)
- [InCommon & Azure AD Article](#)
- [InCommon & Okta Article](#)
- InCommon and GÉANT CAMP Highlights - [Full Presentation \(1 hour 38 minutes\)](#), [Demo of Cirrus Bridge in the Azure AD Console \(7 minutes\)](#)

## General Information - Federated Identity

- [EDUCAUSE 7 Things You Should Know About Federated Identity](#)
- [InCommon Federation Library Confluence Site](#)

## Cirrus Customer Success - Bridge Use Cases

- [CSU Monterey Bay - Campus Access to InCommon & CAS Services with Okta](#)
- [Union College - College Access to InCommon Services with Okta](#)
- [University of Notre Dame - University Access to InCommon & CAS Services with Okta](#)
- [University of Southern Indiana - University Access to CAS Services with Okta](#)
- [Cégep de Trois-Rivières - University Access to Canadian Access Federation Services with Azure AD](#)

# Cirrus Customer Panel

# Kevin Hickey

Director of Information Security, University of Detroit Mercy

## New to InCommon Use Case



## Background

- It had been a goal for the University to join InCommon for years. Lack of internal resources and technical limitations had prevented the project from moving forward.
- In late 2020, the decision was made to consolidate the University's IAM infrastructure into Azure AD. The business drivers included improved reliability, security, and reduced administrative overhead.
- With Azure AD selected as the foundation, we reviewed the potential solutions to integrate Azure AD with InCommon.
- We investigated several in-house options. 1) Utilizing Shibboleth as a SAML proxy. 2) Connecting Shibboleth to a hosted Azure Active Directory Domain Services.
- Cirrus Identity Bridge was a cloud solution that directly integrated with Azure AD. The subscription model allowed the University to quickly move forward with the project.

## Implementation Highlights

- Registering to become a member of InCommon requires signing the participation agreement and completion of an identity proofing process by InCommon. Cirrus Identity assisted us configure our InCommon service.
- Once InCommon membership was completed, configuring the bridge with Azure AD took less than an hour. The bridge can be added from the Azure AD Gallery.
- We set up the default and Research and Scholarship SPs. With these two configurations we were able to immediately connect Educause and PubMed as proof of concept and initial rollout to the community.
- The overall implementation time frame was approximately 90 days. The actual number of implementation hours has been approximately 50 hours so far.

## Lessons Learned

- Working with Cirrus Identity, the process is simpler than you can imagine. It will take longer to process the purchase orders and paperwork then complete the bridge configuration and have live federated sign-ins.
- Build it and they will come. Once you have joined InCommon and configured the Cirrus Bridge the community will find the use cases.
- Don't forget that InCommon offers more than simply federation. Other services include EduRoam, a global wifi roaming service, certificate service, and more.

# Molly McDermott

Sr. Project Manager, Illinois Institute of Technology

## IAM Cloud Consolidation Use Case



**ILLINOIS TECH**

## General

- Illinois Tech decided to implement Okta in December 2021
- We started working with Cirrus in January 2022
- We are still early in our engagement, in the Bridge configuration stage
- Our goal is to go live in early June

## Goal/reason for Implementing the Cirrus Bridge

- We are deploying Okta for our IAM solution and we recognized that Cirrus could be used as a bridge for our applications that do not work natively with Okta for our SSO

## Why was the Cirrus Bridge selected

- The Cirrus Bridge will accelerate the migration of applications from CAS 3/5 and Shibboleth to Okta/Cirrus. In addition, this service was recommended by another university who completed the Okta implementation and successfully used the Cirrus Bridge.



## Implementation Highlights

- Implementation plan from a Project Manager perspective:
  - We are still fairly early in our implementation so far, but we have a clear roadmap and timeline from Cirrus
  - If implementation goes as well as the kick-off process, we should be on track to test our SAML applications next week
  - So far, happy with progress
    - Efficient meetings
    - Very responsive via email
    - Clear expectations of what needs to be done

## Suggestions & Lessons Learned

Suggestions for institutions that are considering implementing the Cirrus Bridge with Okta:

- a. Even before our engagement with Cirrus, and in preparation for our Okta engagement, we did a lot of pre-work in listing out all of our applications / service providers
  - i. we have 87 CAS applications
  - ii. the biggest lift so far was listing out all of the attributes for each application, which required manual effort from our developers
- b. The earlier you can get started with that, the faster the kick-off process can go

# Mike Dulay

Director of Web Tech Services, Millersville University

## IAM Cloud Consolidation Use Case



Millersville University

## Background

Prior to using Cirrus, Millersville had the following goals:

1. Consolidate from 3 SSO solutions to one single IDP
2. Provide a single account and format for authentication. Previously both username and email were used. Our new plan was to use email address UPN.
3. Simplify account management with Azure AD and eliminate syncing multiple directories

A cyber attack caused us to need to quickly move to one single SSO, but we had two issues:

1. We had legacy applications that still needed to use the CAS protocol
2. We also had some InCommon applications that could not integrate with Azure AD

## Implementation Highlights

- Since we had been preparing to merge IDPs, we had a list of all attributes being used for each SP. This saved us time!
- A few weeks after the cyber attack we were up and running thanks to Cirrus Support. We would not recommend this path, but it was helpful to focus resources with a new network.
- Restoring our applications and servers took quite a long time. It was beneficial to save SSO resources.
- Not all of our applications go through the Bridges. We made it a priority to bring up applications that could use SAML directly on Azure AD. That left about a dozen that used the InCommon SAML Bridge and/or the CAS Bridge.

## Lessons Learned

- Start taking inventory now, even if it will be a while before you would switch. Having inventory on hand of all SPs, their attributes and whether they were federated was valuable
- Make a priority list of applications and servers to restore in case of a disaster, it will help you restore if ever needed!
- If you have a mixed environment of SSO and IDPs, start planning where you would like to be. It might not be something that can happen overnight - we had been preparing for a couple of years and working through the process.
- See if your current IDP can extend to use protocols that might be older like CAS for your legacy applications

## Lessons Learned Continued

- Make sure you have support for your current and future IDP - you don't know when you will need it. We were ending our contract with our previous IDP solution and didn't have the support we needed, so it took a lot of our staff resources to make things work
- From my experience, Cirrus Support has been exceedingly quick and helpful

# Questions & Answers



# Stay Tuned for More Webinars!



If you would like to hear more about the Cirrus Bridge,  
please email [sales@cirrusidentity.com](mailto:sales@cirrusidentity.com)!



**cirrus** identity

**Dedra Chamberlin,**  
**CEO**  
dedra@cirrusidentity.com

**Mark Rank,**  
**Director of Product**  
mark.rank@cirrusidentity.com

**Patrick Radtke,**  
**CTO**  
patrick@cirrusidentity.com

**Kristina Deaton,**  
**Director of Customer Success**  
kristina@cirrusidentity.com

**Karen Kato,**  
**Director of Sales & Marketing**  
karen@cirrusidentity.com

## Large R1 Universities



## Small to Mid-Size Colleges



## Higher Ed Institutions



Customers Love Us



Blackboard



Shibboleth.



## Product Integrations

- Accelerate ERP Implementations
- Reduce custom software requirements
- Eliminate business process re-engineering
- Federation

# Cirrus Solutions Make it Easy to Streamline Access:



## Single Sign-On

Unify single sign-on for your students, faculty, and staff as well as “external” users. Make it easy for applicants using [Slate](#) and/or alumni using [Salesforce](#) too! Retire on-prem solutions like CAS and free up your IAM team to work on higher priority projects.



## InCommon / EduGAIN

The Cirrus multilateral federation adapter Bridge will enable your commercial Identity Provider ([Azure AD](#), [Okta](#), [Google](#) or others) to connect to [InCommon](#), [CAF](#) or the [UKFederation](#) - all worldwide [eduGAIN](#) federations!



## Share Services

Allow access to online services and applications from multiple identity providers. Great for [InCommon](#) service providers or institutions with multiple campuses or medical schools!



## Social Logins

Applicants, parents, online learning guests or alumni can use a username & password they already have and know! Reduce support and licensing by not having them in your core identity management systems!



## Hosted Identities

Provide strategic users an account branded to your institution. Great solution for independent researchers and for users that don't have or don't want to use social login!

# Cirrus Solutions - Your Swiss Army Knife of Identity & Access Tools!



## Gateway

Allows applicants, parents, alumni, suppliers, retirees or other guests to authenticate with their social login ([Google](#), [Microsoft](#), [LinkedIn](#), [Facebook](#), [Twitter](#), [Amazon](#)) in your institution's single sign-on (SSO) environment.



## Account Linking

Links identifiers and attributes for users that don't need a username/password in your core identity provider to other identifiers. Supports one username and password with many identifiers and facilitates the transitions from applicant to student to alumni.



## Invitation

Customers can use pre-built web forms or APIs for workflow allowing authorized users to sponsor a guest invitation. Supports email invitations, claim process, acceptance of terms and setup. Custom data can be included on the web form and API call.



## Identity Provider Proxy

Provides a single identity provider endpoint where service provider(s) integrate with multiple identity providers. The proxy also supports sophisticated attribute translations required for authentication or authorization. Also supports [SAML](#) to [CAS](#) protocol translation.



## Bridge

Provides a federation adapter that supports [Azure AD](#), [Okta](#), [Google](#) and other commercial identity providers to connect to services provided through [InCommon](#) and all [eduGAIN](#) federations. Also supports [SAML](#) to [CAS](#) protocol translations and converts [Slate](#) into a SAML IdP.



## OrgBrandedID

An option for research organizations that need an Identity Provider of Last Resort and a solution for users that don't have or want to use a social login! The login is branded to your institution and hosted by Cirrus. Cirrus provides user self-service password management.



## MyResearchID

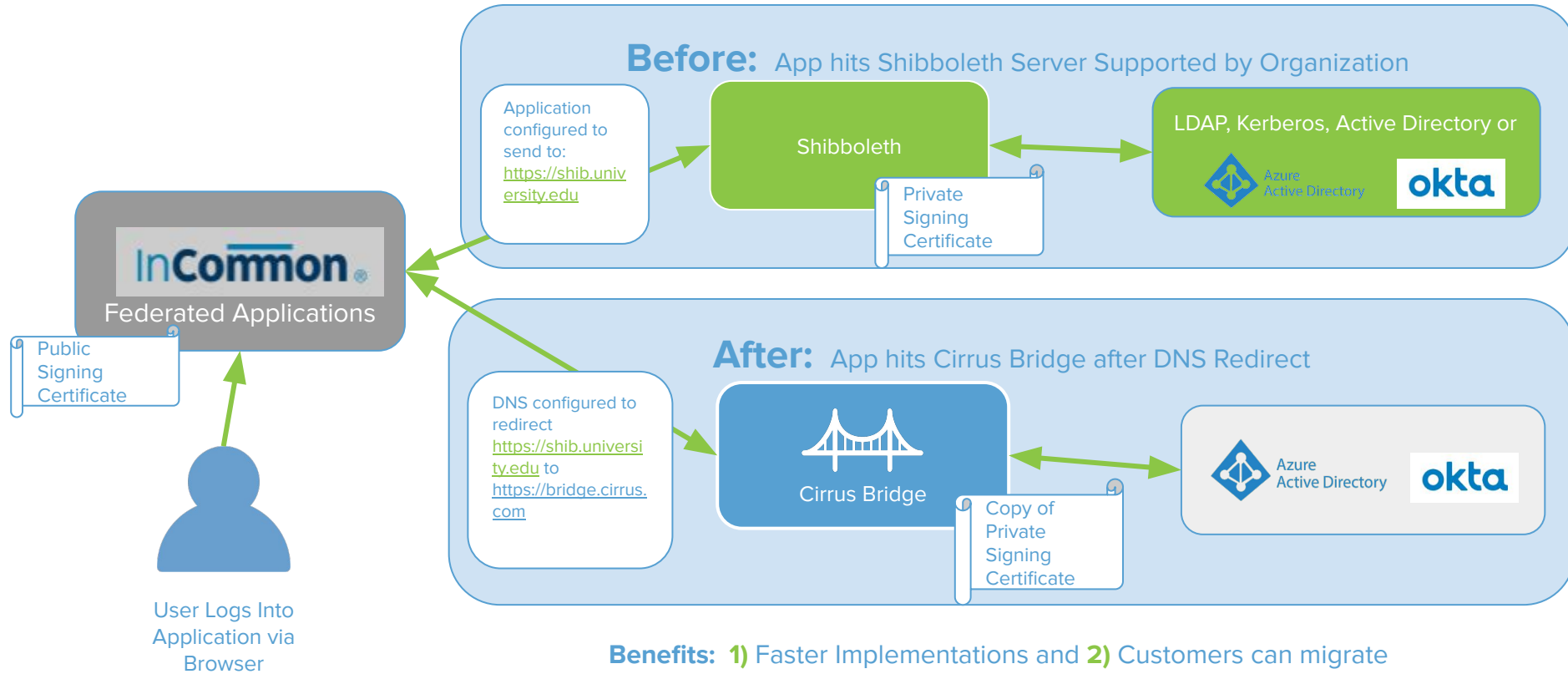
Provides an easy-to-use, externally hosted SAML2 compliant identity for researchers to use across institutions.



## EduAccessID

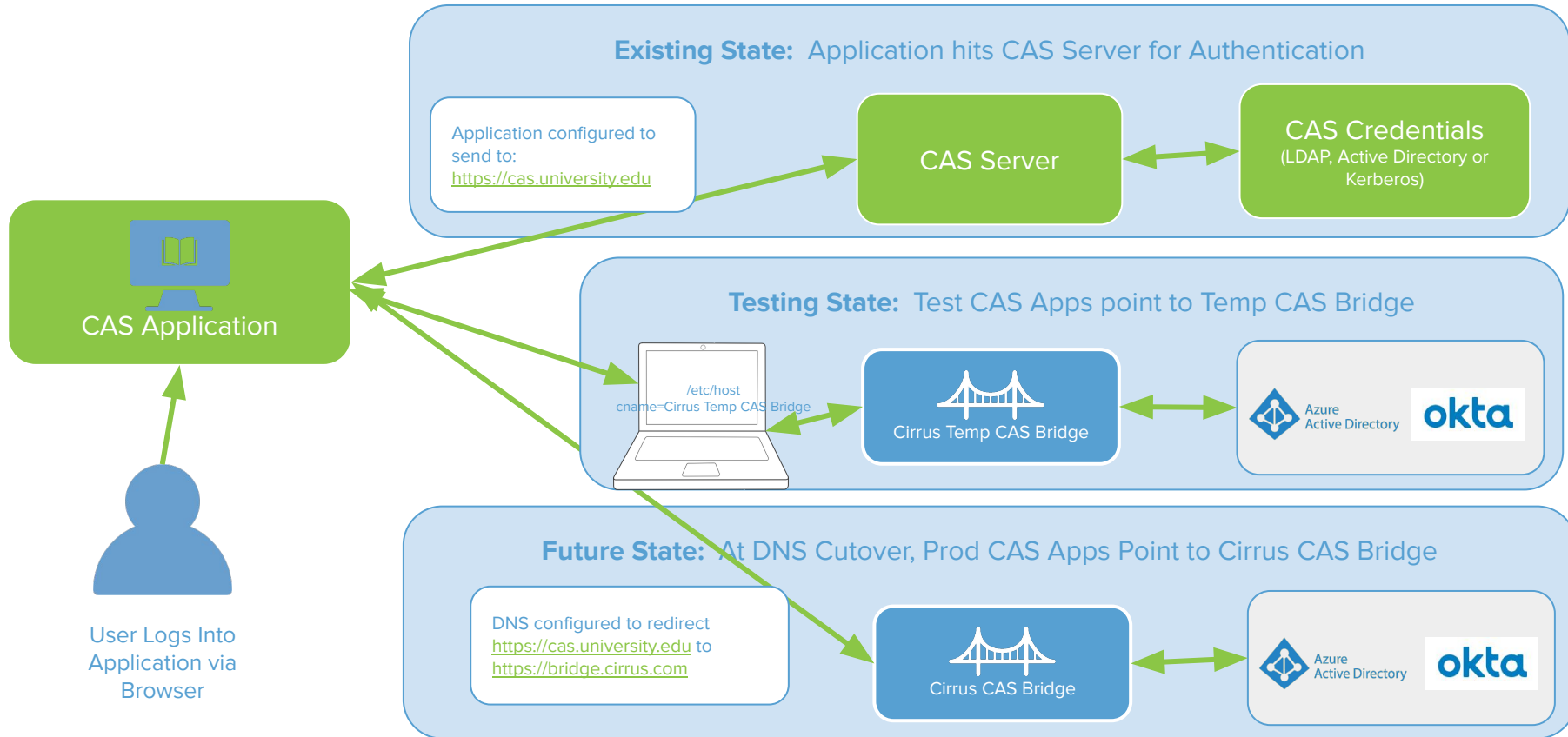
Provides a self-service, externally hosted SAML2 compliant identity for collaborators to use across institutions when they don't have or want to use a social login.

# Cirrus DNS Add-On for SAML - High Level Architecture



**Benefits:** 1) Faster Implementations and 2) Customers can migrate from Shibboleth to the Cirrus Bridge without making changes in the InCommon Federation Manager application

# Cirrus DNS Add-On for CAS - High Level Architecture

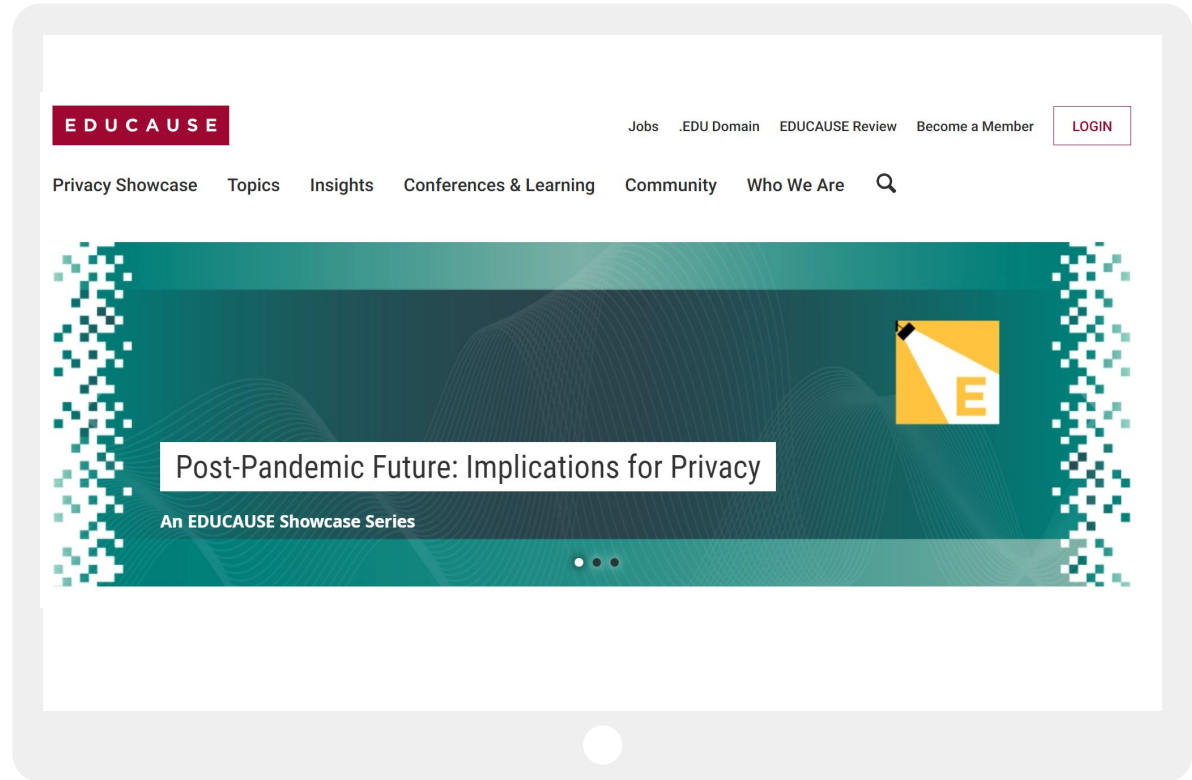


**Benefits:** Faster Implementations and consolidation to commercial SSO solutions



## Customer Demonstration

<https://www.educause.edu/>



# Cirrus Bridge Customers

- American University at Sharjah\*
- [California State Monterey Bay](#)
- [Cegep de Trois-Rivieres\\*](#)
- Chapman University\*
- Digital Theatre
- EDUCAUSE\*
- Icahn School of Medicine at Mount Sinai
- Iowa State University
- Mansfield University\*
- Millersville University\*
- Lock Haven University\*
- Oregon Institute of Technology\*
- Pomona College\*
- The University of Tampa
- [Union College](#)
- University of Louisville\*
- University of Nevada, Las Vegas
- [University of Notre Dame](#)
- University of Rhode Island\*
- University of Puget Sound
- West Point United States Military Academy\*

