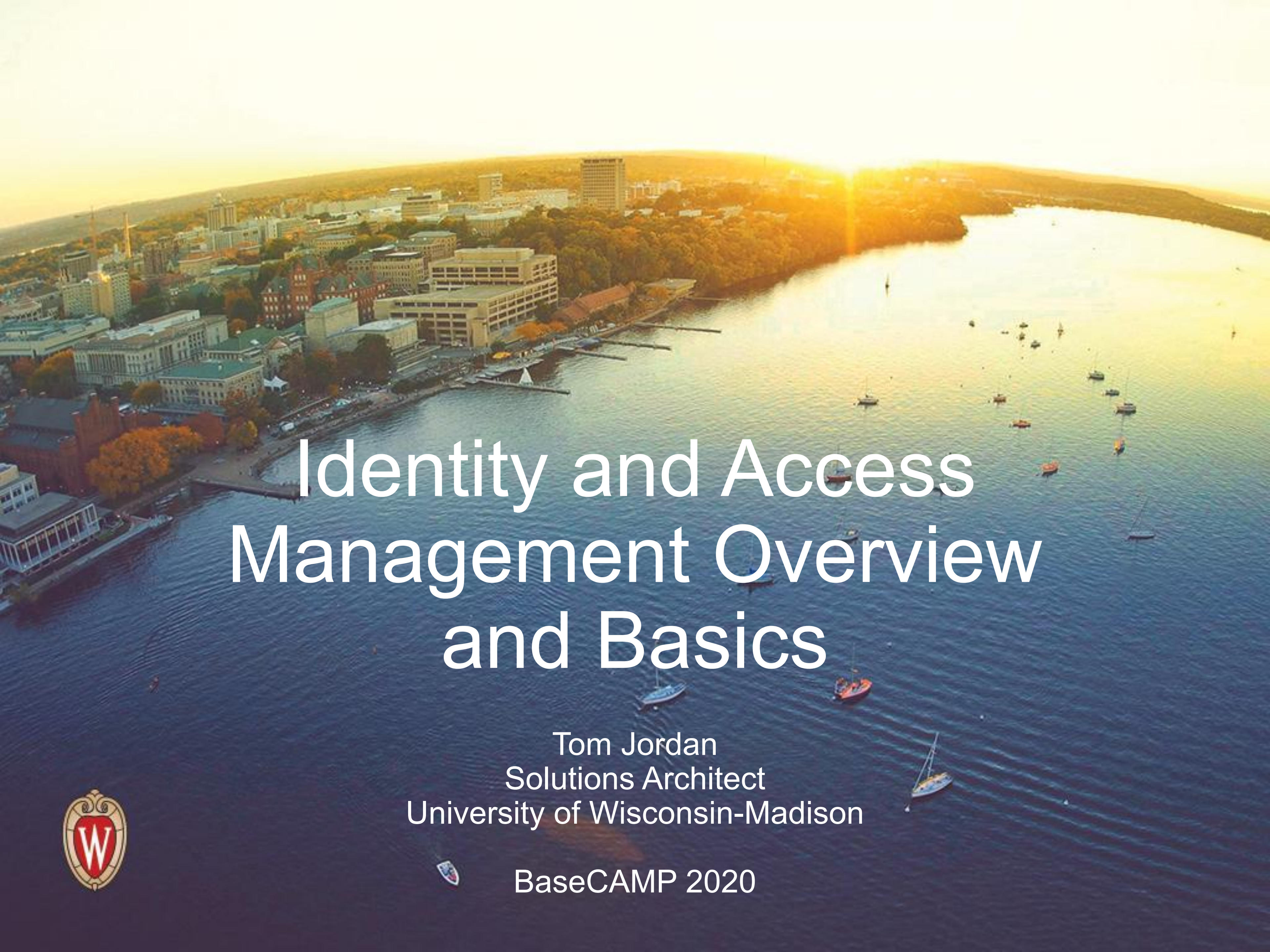


Identity and Access Management Overview and Basics

Tom Jordan
Solutions Architect
University of Wisconsin-Madison

BaseCAMP 2020

Agenda

- Welcome to the community!
- The Higher Ed IAM Landscape
- Essential functions of an IAM Practice - Overview
- Community Engagement! (your questions here..)
- Essential functions of an IAM Practice - In Greater Detail
- Trends and Future Directions

Tom Jordan Bio

- Integration Architect at University of Wisconsin-Madison
- Reference Architecture Lead for TIER Initiative
- Contributor - Entity Registry and Data Structures Working Groups
- Chair - CACTI (Community Architecture Council for Trust and Identity)
- Proud member of Higher Ed IAM community!

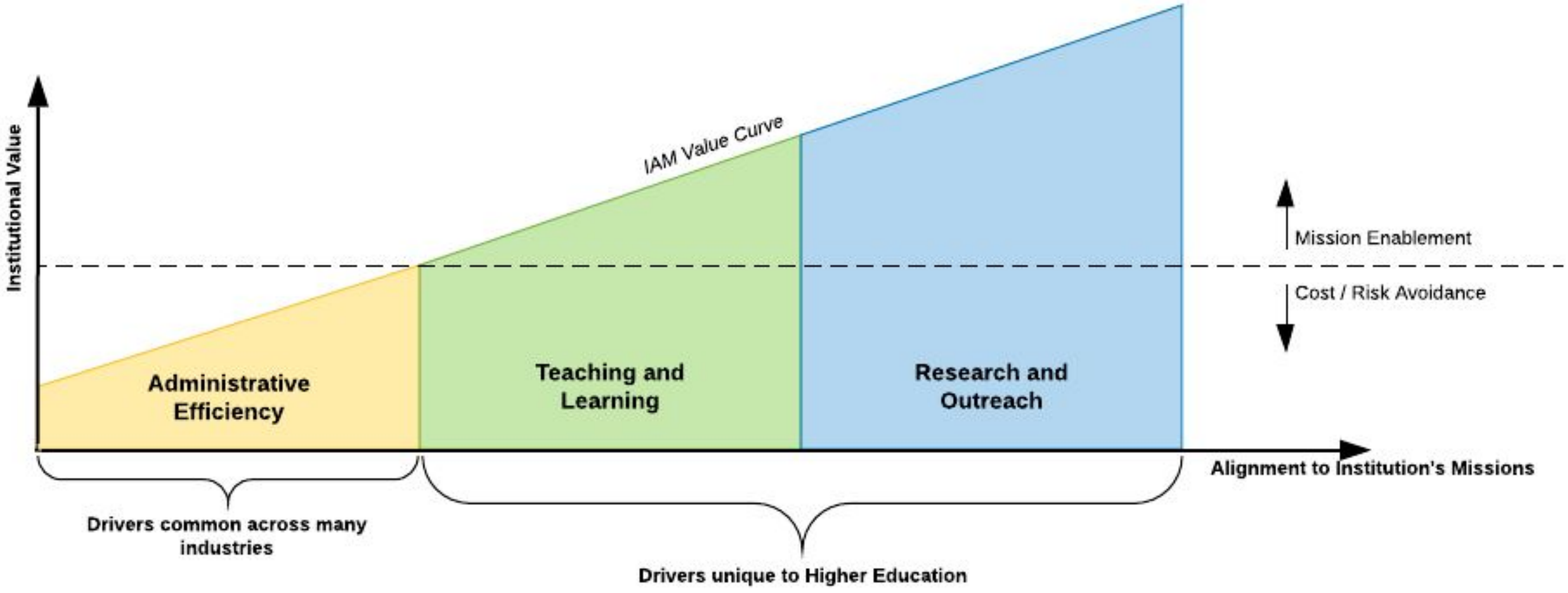
IAM as a Practice in Higher Education

Commonalities with Commercial IAM

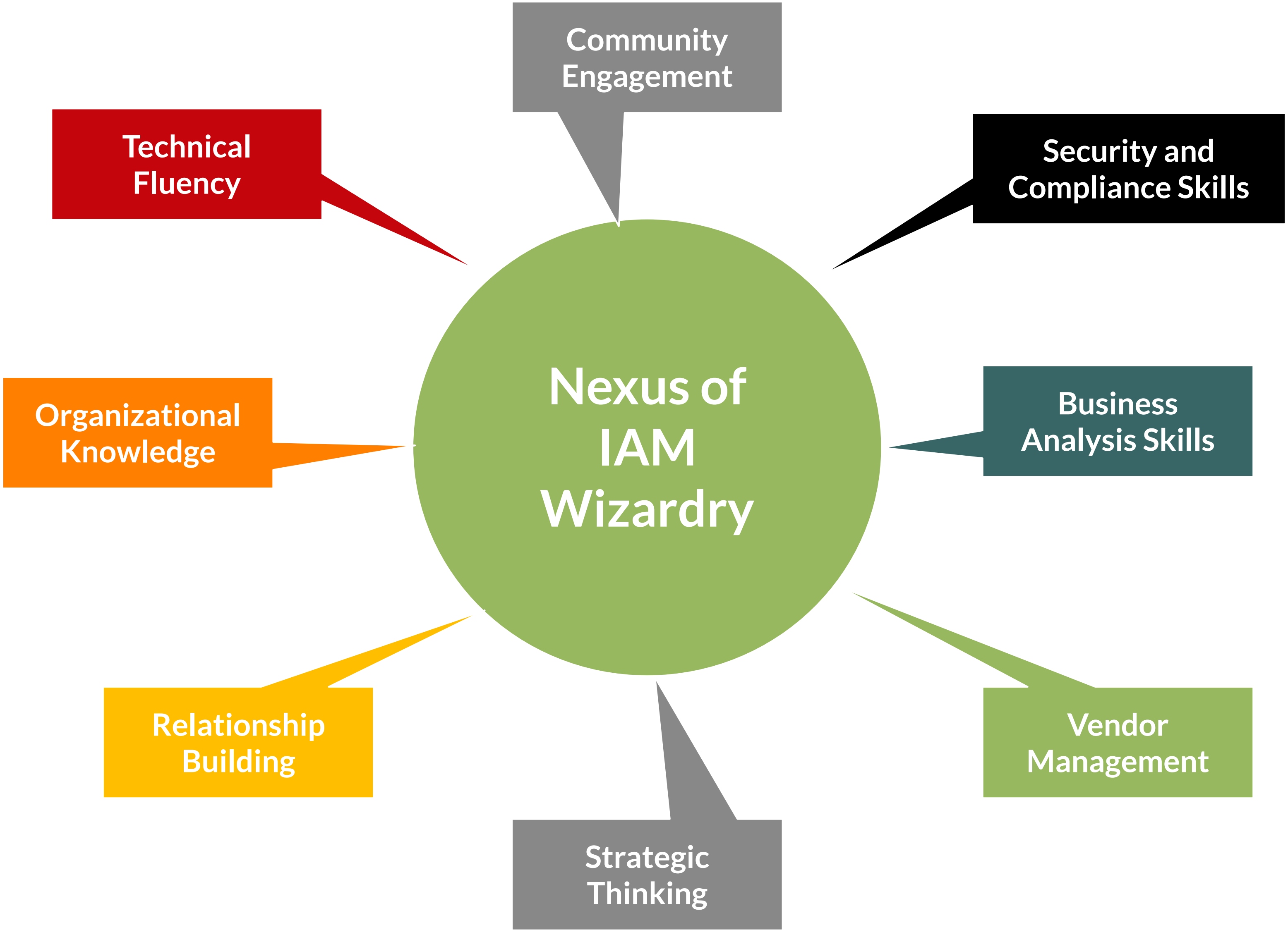
- Identity Governance
- Certification and Compliance
- Mostly cost and risk avoidance

Drivers Unique to Higher Education

- Fuzzy borders
- Distributed Constituencies
- Cross-institutional Collaborations
- Mission-focused activities



The Higher Ed IAM Practitioner



Nexus of IAM Wizardry

Community Engagement

Security and Compliance Skills

Business Analysis Skills

Vendor Management

Strategic Thinking

Relationship Building

Organizational Knowledge

Technical Fluency

A few quick polls

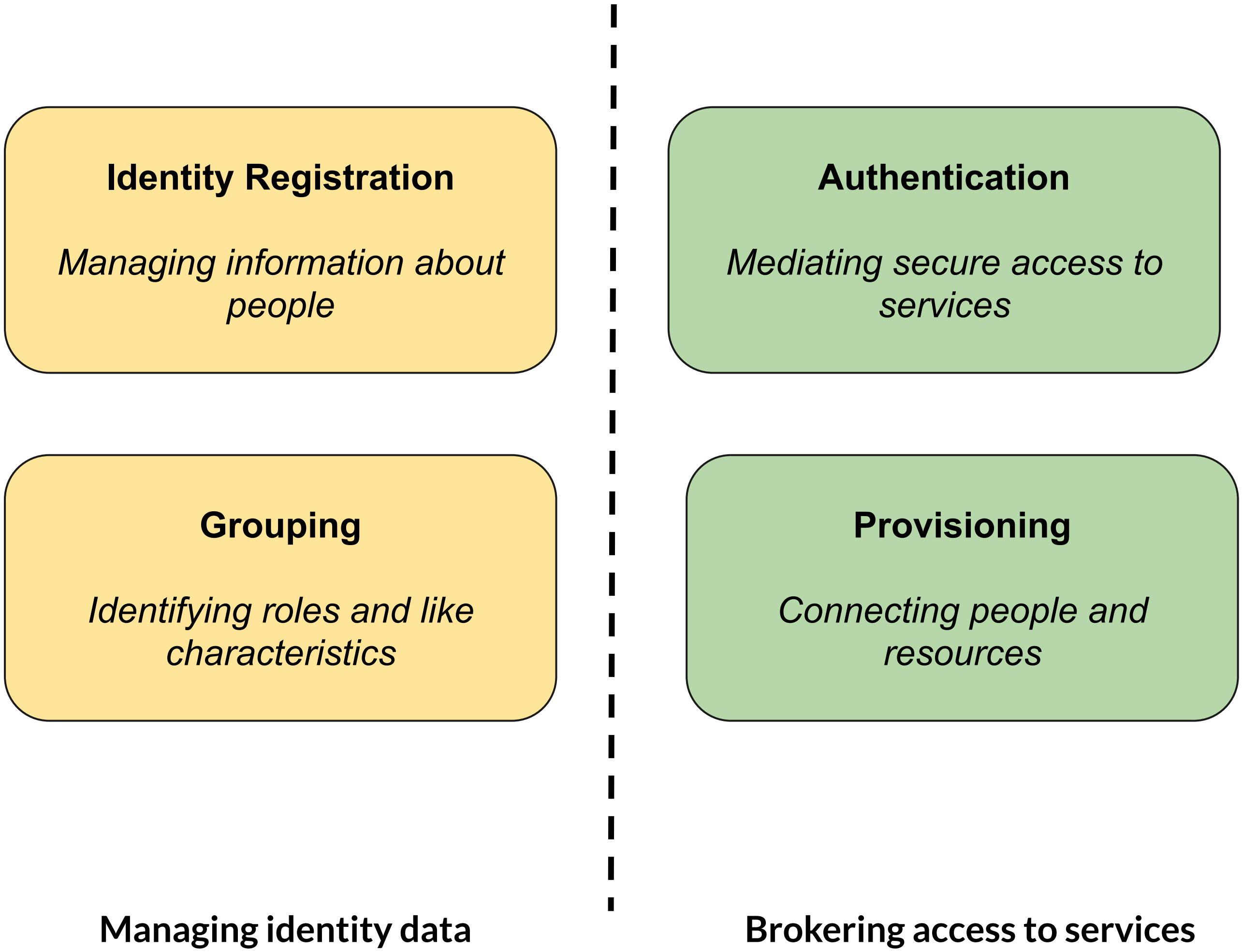
Poll #1 - How long have you worked in Higher Education

- 0-3 years
- 3-5 years
- 5-10 years
- More than 10 years
- I don’t work in Higher Education

Poll #2 - How long have you worked in Identity and Access Management?

- 0-3 years
- 3-5 years
- 5-10 years
- More than 10 years

Essential Functions of an IAM Practice



Identity Registration

Managing information about people

Grouping

Identifying roles and like characteristics

Authentication

Mediating secure access to services

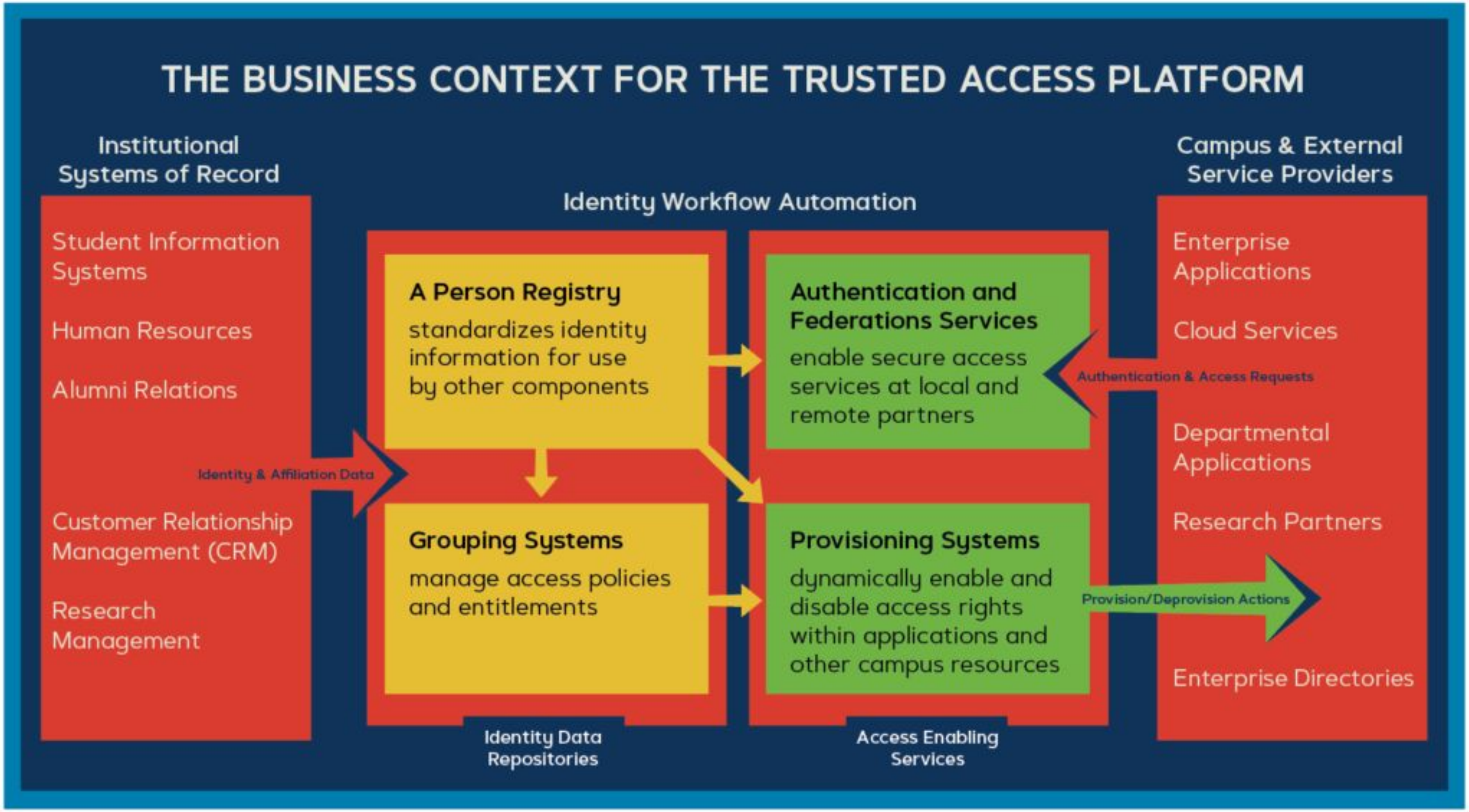
Provisioning

Connecting people and resources

Managing identity data

Brokering access to services

Trusted Access Platform Architecture



THE BUSINESS CONTEXT FOR THE TRUSTED ACCESS PLATFORM

Institutional Systems of Record

Student Information Systems

Human Resources

Alumni Relations

Customer Relationship Management (CRM)

Research Management

Identity Workflow Automation

A Person Registry
standardizes identity information for use by other components

Grouping Systems
manage access policies and entitlements

Identity Data Repositories

Authentication and Federations Services
enable secure access services at local and remote partners

Provisioning Systems
dynamically enable and disable access rights within applications and other campus resources

Access Enabling Services

Campus & External Service Providers

Enterprise Applications

Cloud Services

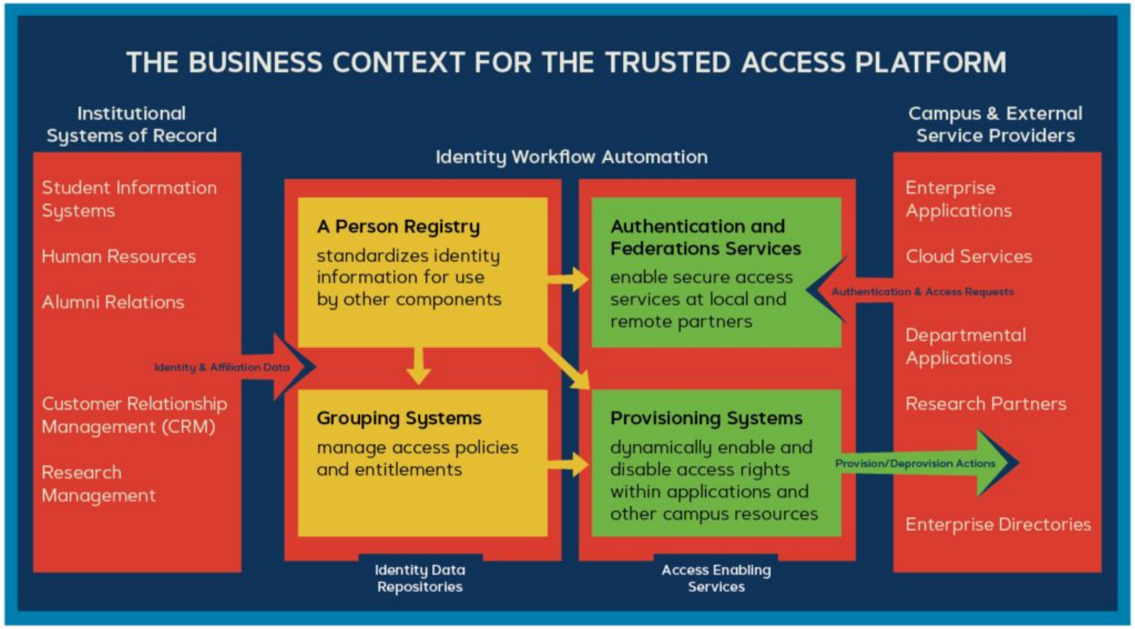
Departmental Applications

Research Partners

Enterprise Directories

Identity & Affiliation Data
Authentication & Access Requests
Provision/Deprovision Actions

Group Time (20 Minutes)



THE BUSINESS CONTEXT FOR THE TRUSTED ACCESS PLATFORM

Institutional Systems of Record

Student Information Systems

Human Resources

Alumni Relations

Customer Relationship Management (CRM)

Research Management

Identity Workflow Automation

A Person Registry
standardizes identity information for use by other components

Grouping Systems
manage access policies and entitlements

Identity Data Repositories

Authentication and Federations Services
enable secure access services at local and remote partners

Provisioning Systems
dynamically enable and disable access rights within applications and other campus resources

Access Enabling Services

Campus & External Service Providers

Enterprise Applications

Cloud Services

Departmental Applications

Research Partners

Enterprise Directories

Identity & Affiliation Data
Authentication & Access Requests
Provision/Deprovision Actions

In your breakout rooms:

- Meet your colleagues!
- Describe how your institution accomplishes these functions
- Identify your core challenges
- Identify the core questions you'd like to get answered at BaseCAMP

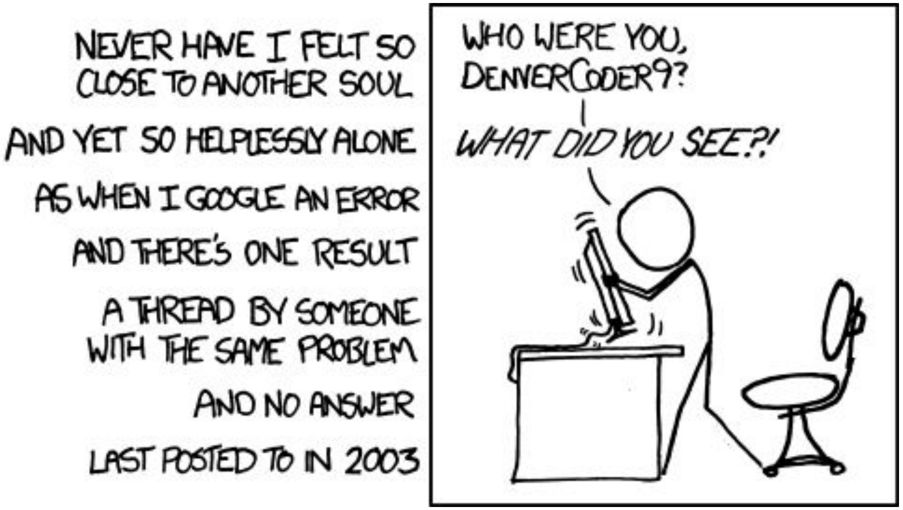
Post your comments in chat, and we'll review as the conference progresses!

Group Review

Common themes? Areas of Divergence?

Please feel free to add questions via chat as the conference progresses..

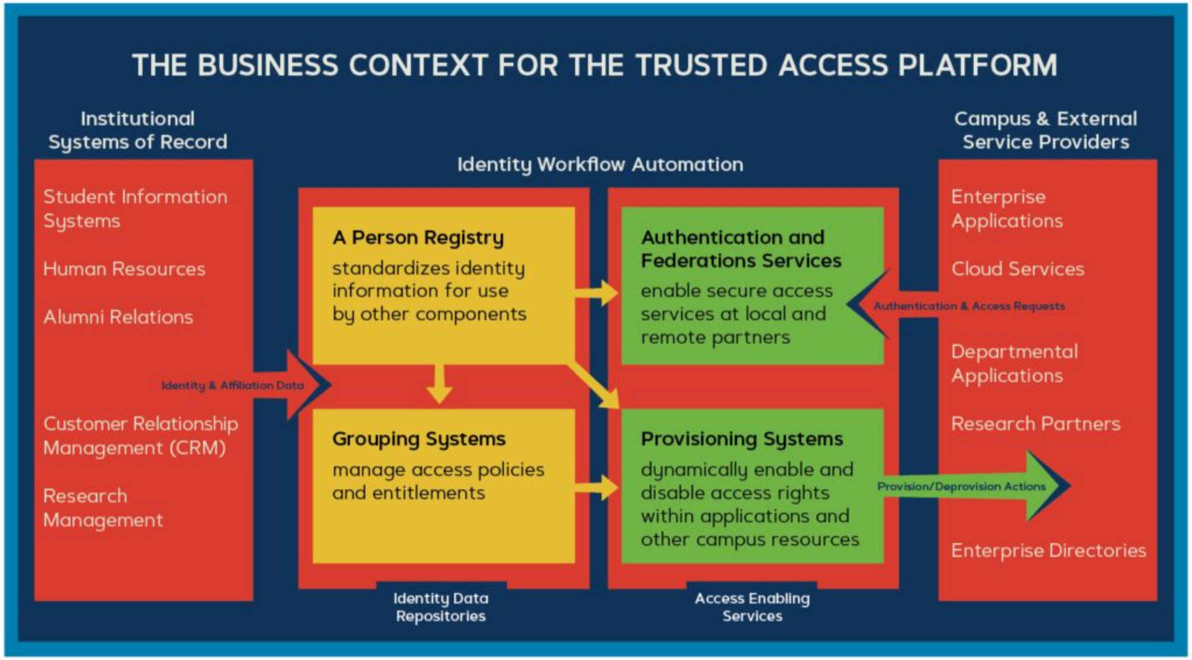
And remember - we’re all in this together!


NEVER HAVE I FELT SO CLOSE TO ANOTHER SOUL
AND YET SO HELPLESSLY ALONE
AS WHEN I GOOGLE AN ERROR
AND THERE'S ONE RESULT
A THREAD BY SOMEONE WITH THE SAME PROBLEM
AND NO ANSWER
LAST POSTED TO IN 2003
WHO WERE YOU, DENVERCODER9?
WHAT DID YOU SEE?!

Let’s Dive In!

In a little bit more detail..

- Identity registries and person repositories
- Grouping
- Provisioning
- Authentication and Federation



THE BUSINESS CONTEXT FOR THE TRUSTED ACCESS PLATFORM

Institutional Systems of Record

Student Information Systems

Human Resources

Alumni Relations

Customer Relationship Management (CRM)

Research Management

Identity & Affiliation Data

Identity Workflow Automation

A Person Registry standardizes identity information for use by other components

Grouping Systems manage access policies and entitlements

Authentication and Federations Services enable secure access services at local and remote partners

Provisioning Systems dynamically enable and disable access rights within applications and other campus resources

Identity Data Repositories

Access Enabling Services

Campus & External Service Providers

Enterprise Applications

Cloud Services

Authentication & Access Requests

Departmental Applications

Research Partners

Provision/Deprovision Actions

Enterprise Directories

Identity Registries and Person Repositories

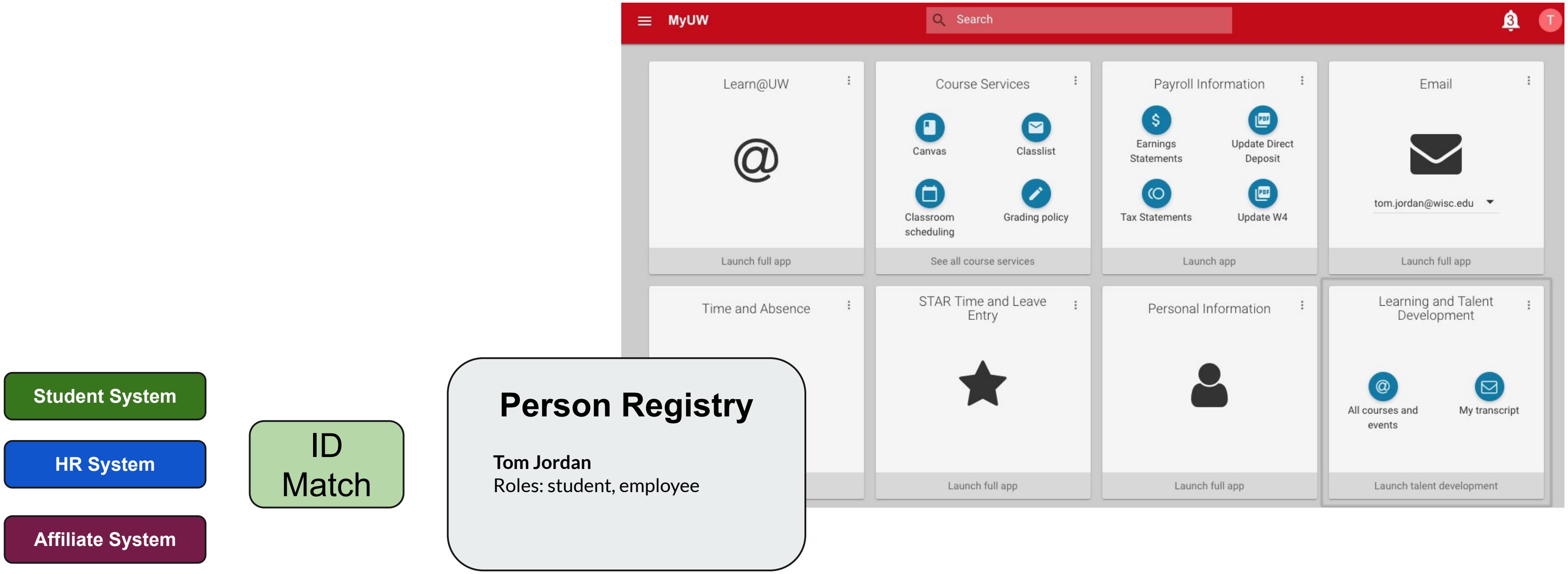
Concepts to cover:

- Aggregating person data
- Person matching and deduplication
- Repositories (directories, databases, MDM)
- Identity Proofing and Credentialing

Identity Registries and Person Repositories

Aggregating person data - Person Registry Function

- Multiple sources
- Identity matching functions
- Single person, multiple roles
- Services based on sum of roles



Student System

HR System

Affiliate System

ID Match

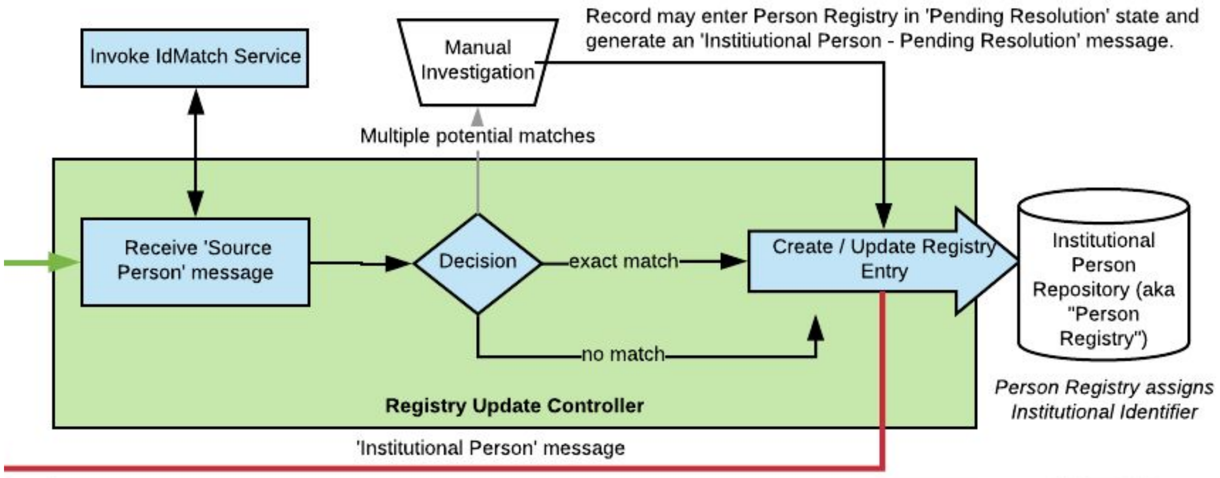
Person Registry

Tom Jordan
Roles: student, employee

Identity Registries and Person Repositories

Person Matching and Deduplication

- Demographic comparison
  - Data quality
  - Privacy
- Continuity-based (‘identity first’)
  - BYOI (Bring Your Own Identity)
- Duplicate detection and remediation
  - Timing (pre-commit vs. post-commit)
  - Joins
  - Splits



Invoke IdMatch Service

Manual Investigation

Record may enter Person Registry in 'Pending Resolution' state and generate an 'Instituional Person - Pending Resolution' message.

Multiple potential matches

Receive 'Source Person' message

Decision

exact match

no match

Create / Update Registry Entry

Institutional Person Repository (aka "Person Registry")

Person Registry assigns Institutional Identifier

Registry Update Controller

'Institutional Person' message

Identity Registries and Person Repositories

Person Repositories

- Directories (LDAP, Active Directory)
- Databases
- Data virtualization and synchronization
- Identity Master Data Management (MDM)
- Thick vs. Thin registries

Where does your organization consolidate identity data?

Banner® by Ellucian

ORACLE® PEOPLESOFT

Active Directory

OpenLDAP

COmanage™

midPoint

salesforce.org

Identity Registries and Person Repositories

Identity proofing

- Identity Assurance Levels (IAL)
  - IAL1 - Self-asserted identity information
  - IAL2 - Verified with moderate confidence
  - IAL3 - Verified with strong confidence
- Binding to credential issuance
- Relation to Authentication Assurance Level (AAL)
- Relation to Federation Assurance Level (FAL)
- Guest systems

Social and external login

- Conveying and consuming assurance levels
- Managing binding to local identity

"On the Internet, nobody knows you're a dog."

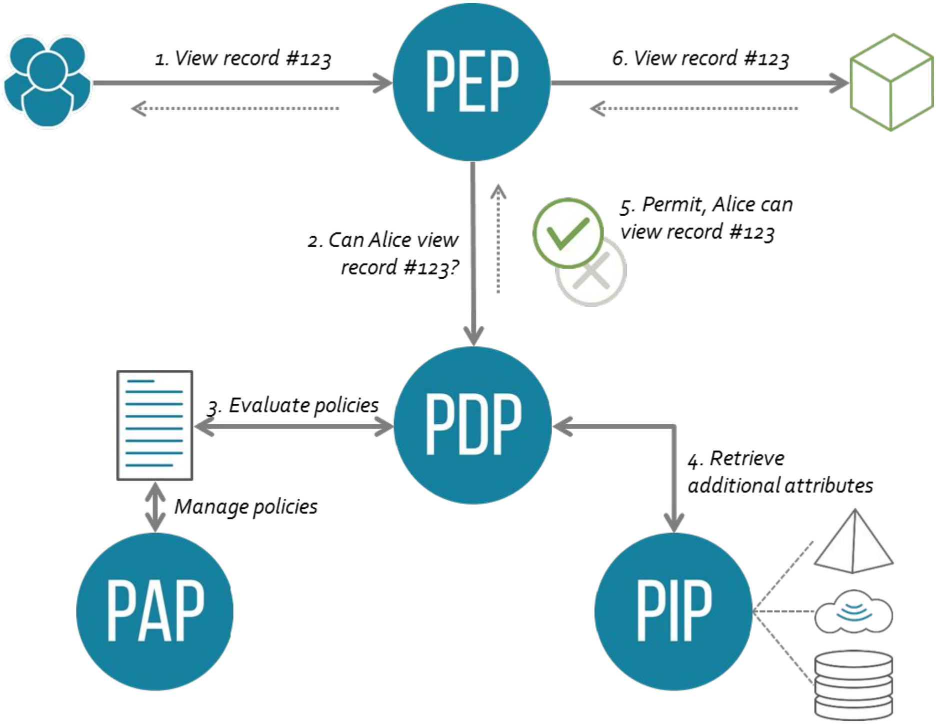
Grouping

Concepts to cover:

- How grouping relates to an access management strategy
- Role-based access control (RBAC) and Attribute-based access control (ABAC)
- Institutionally Meaningful Cohorts vs. Access Policy Rules
- Grouping in concert with access management

Grouping

- Access Management Concepts
  - Policy Enforcement Point (**PEP**)
  - Policy Decision Point (**PDP**)
  - Policy Administration Point (**PAP**)
  - Policy Information Point (**PIP**)
- Role-Based Access Control (RBAC)
- Group Memberships as attributes (ABAC)
- Grouping as a function
  - Defines logical cohorts
  - Aids in policy administration
  - Produces **subject attributes** for policy decision and enforcement

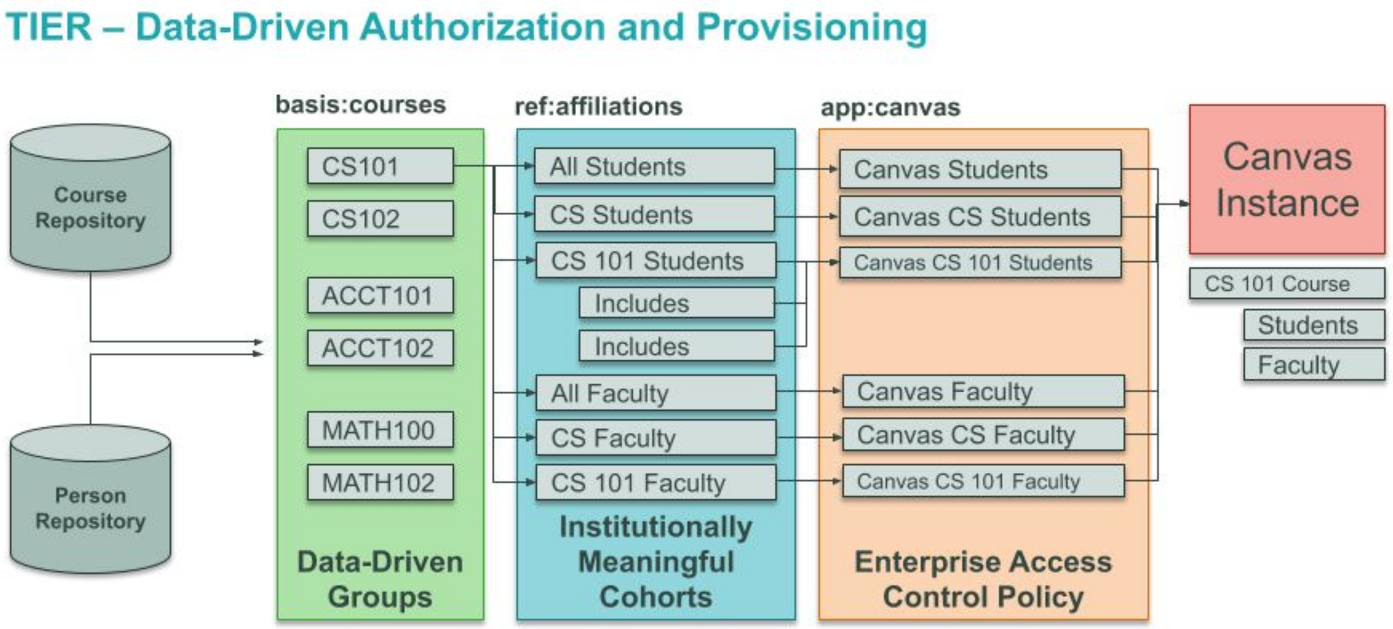

1. View record #123
PEP
6. View record #123
2. Can Alice view record #123?
5. Permit, Alice can view record #123
3. Evaluate policies
PDP
4. Retrieve additional attributes
Manage policies
PAP
PIP

Grouper Deployment Guide:
https://spaces.at.internet2.edu/display/Grouper/Grouper+Deployment+Guide

Grouping

Key concepts:

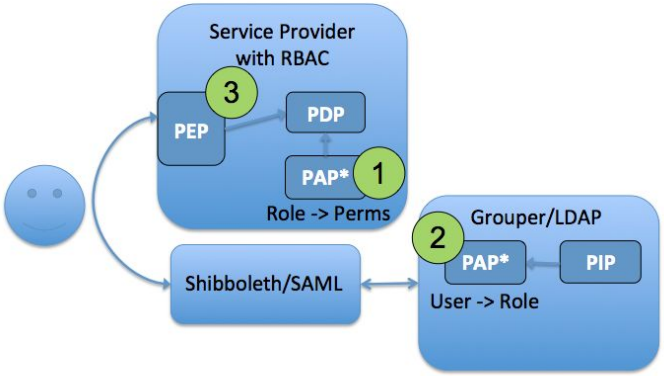
- Data-driven groups
- Institutionally Meaningful Cohorts
- Enterprise Access Control Policy
- Natural policy language
- Manage by exception



Grouping

Grouping in concert with access management:

- Institutional roles map to access policies
- Access policy groups (coarse-grained entitlements) provided by IAM infrastructure
- Fine-grained permissions managed within the service provider (application)



There are a variety of access control models (ACMs) that can be used based on application needs and limitations. The right ACM for a given situation is driven largely by business need and application constraints.

Brief Intermission

Let’s take a 10 minute break..

- Stretch
- Snack
- Synthesize!

Remember: keep posting those questions in chat!

Provisioning and Deprovisioning

Concepts to cover:

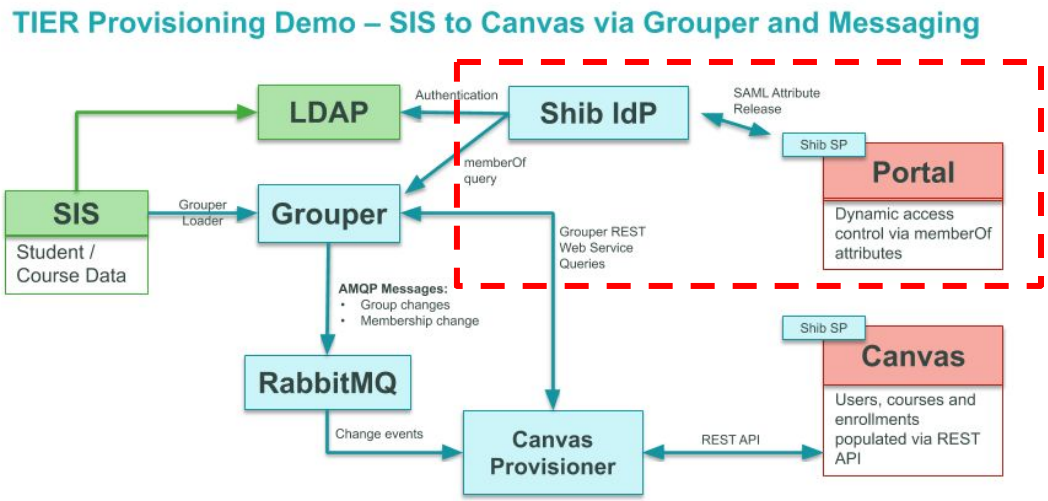
- “Just in Time” vs. “Just in Case” provisioning
- Rule-based vs. request-based provisioning
- Declarative models and exception reporting
- Attestation

Poll question: Who feels like they’ve got deprovision under control?

Provisioning and Deprovisioning

“Just In Time” (JIT) Provisioning

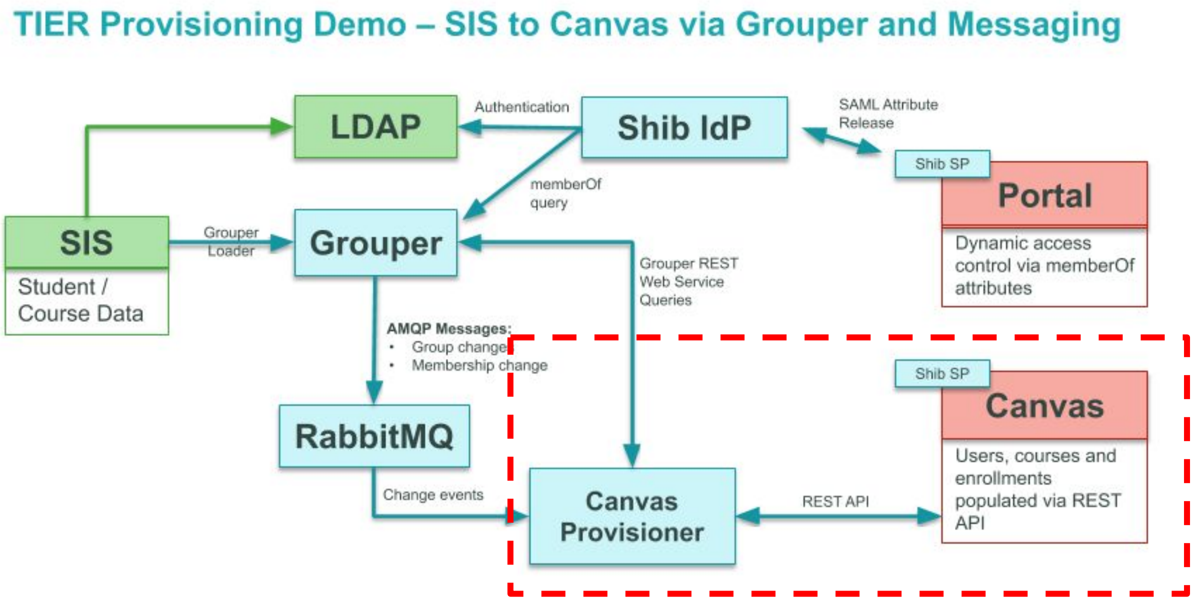
- Provisioning at user login
- Data delivery via attribute release
- Deprovisioning via inactive purge
- (+) Minimal data footprint
- (+) Loose coupling between app and infrastructure
- (-) Challenging to grant permissions pre-login
- (-) Audit strategies


TIER Provisioning Demo – SIS to Canvas via Grouper and Messaging

Provisioning and Deprovisioning

"Just In Case" (JIC) Provisioning

- Provisioning at user eligibility
- Data delivery via provisioning agent
- Deprovisioning via active means
- (+) Pre-login access mgmt
- (+) Bi-directional audit / rogue detection
- (+) Audit comfort
- (-) Tight coupling
- (-) Scale
- (-) Timeliness



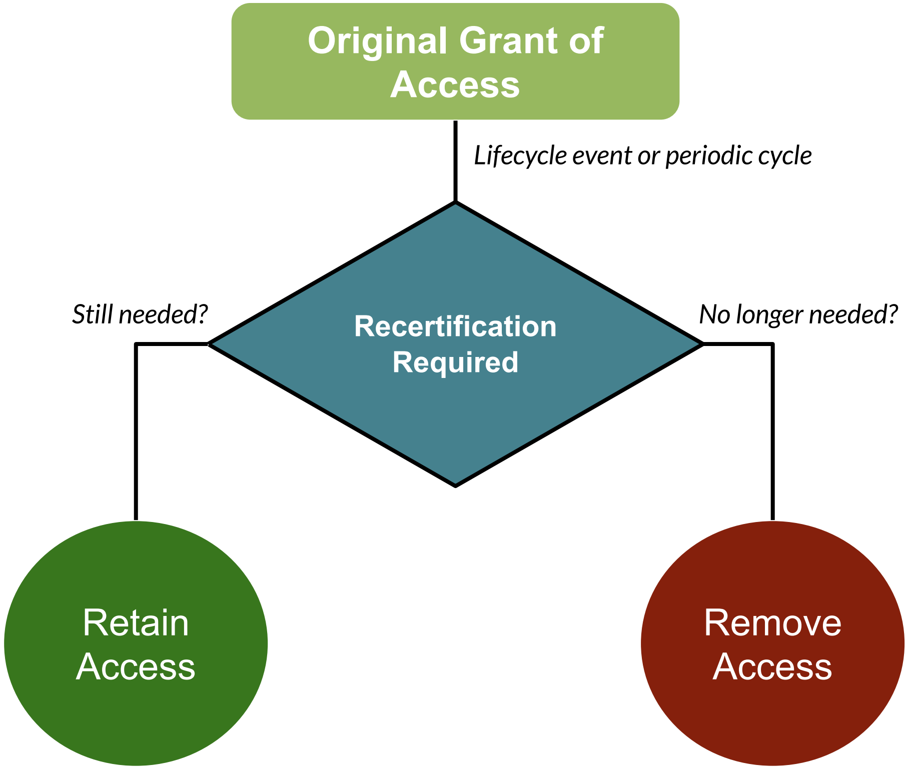
Provisioning and Deprovisioning

Declarative provisioning models:

- Attestation / Certification
- Bi-directional audit / rogue detection
- Privileged Access Management (PAM)

Cloud provisioning

- Google
- Azure / O365
- Cisco Spark
- Amazon



Authentication and Federation

Concepts to cover:

- Directory-based authentication (LDAP, AD, RADIUS)
- Web SSO technologies
- Multi-Factor Authentication
- Attribute delivery
- Federation
- Futures

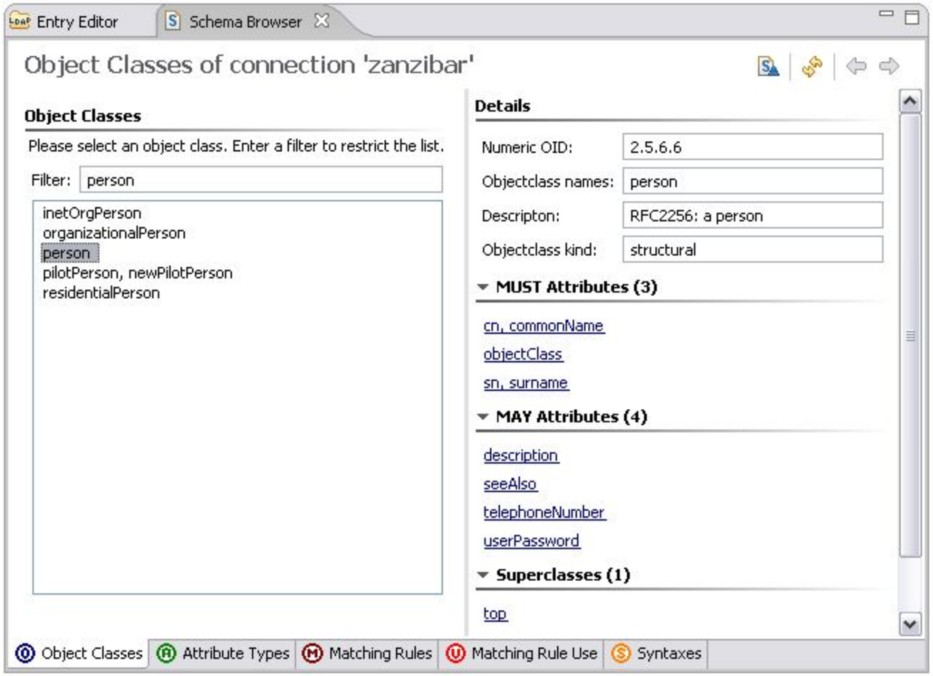
Authentication and Federation

Directory-based authentication

- LDAP
- Active Directory
- RADIUS

Common Directory Schema:

- orgPerson / inetOrgPerson
- eduPerson
  - eduPersonAffiliation
  - eduPersonEntitlement
- SAML attributes
- OAuth and OpenID profiles



Object Classes of connection 'zanzibar'

Object Classes

Please select an object class. Enter a filter to restrict the list.

Filter: person

inetOrgPerson
organizationalPerson
person
pilotPerson, newPilotPerson
residentialPerson

Details

Numeric OID: 2.5.6.6
Objectclass names: person
Descripton: RFC2256: a person
Objectclass kind: structural

MUST Attributes (3)

cn, commonName
objectClass
sn, surname

MAY Attributes (4)

description
seeAlso
telephoneNumber
userPassword

Superclasses (1)

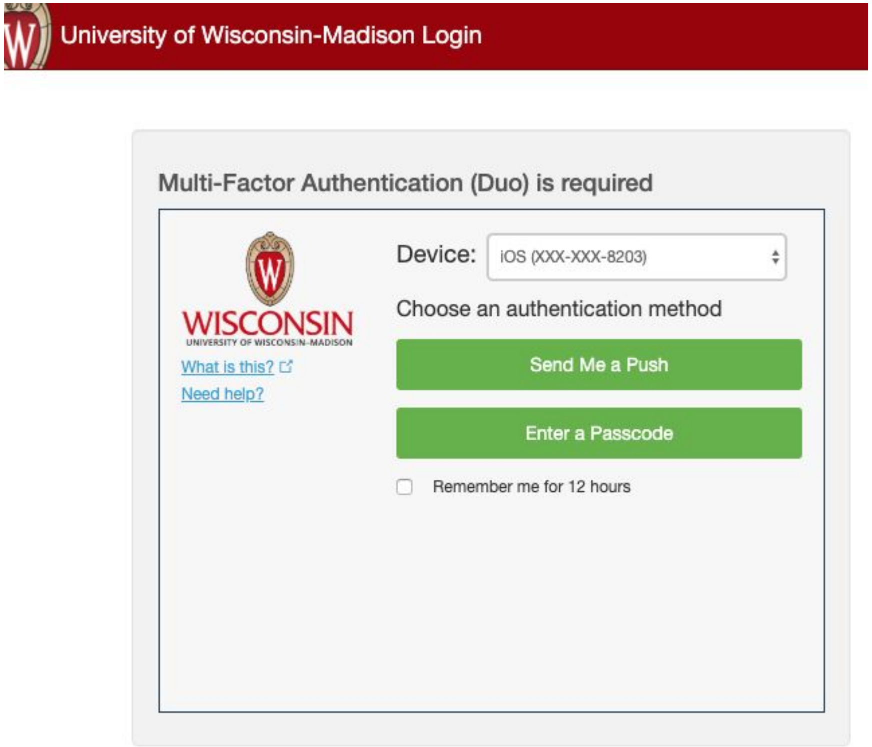
top

Authentication and Federation

Authentication Assurance Level (AAL)

Multi-Factor Authentication Technologies

- Token-based (OTP, Fido / U2F)
- Push
- WebAuthN
- Touch ID



University of Wisconsin-Madison Login

Multi-Factor Authentication (Duo) is required

Device: iOS (XXX-XXX-8203)

Choose an authentication method

☐ Remember me for 12 hours

Authentication and Federation

Web single sign-on (SSO) entities

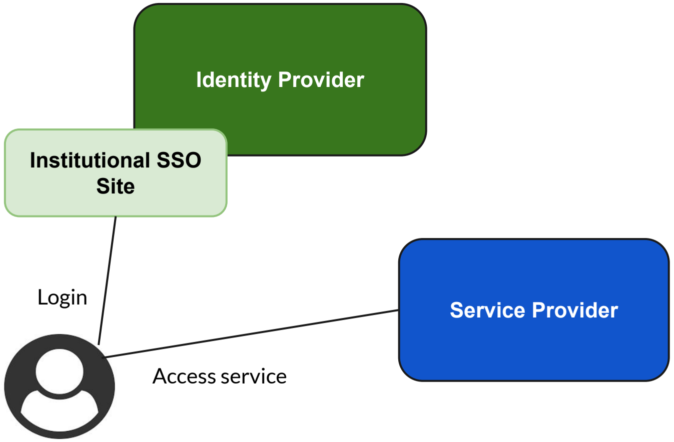
- Identity Provider (IdP) / Authorization Server
- Service Provider (SP) / Resource Owner

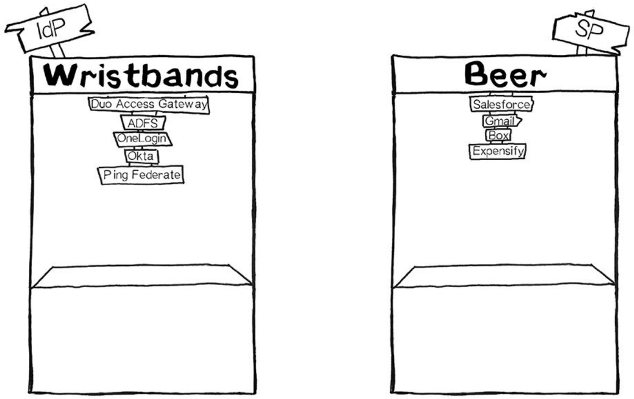
Important Functions

- Authentication
- Authorization
- Attribute Release
  - Consent!

Important Technologies

- SAML2
- Ws-Fed
- OAuth2 / OpenID Connect
- Active Directory Federation Services (ADFS)



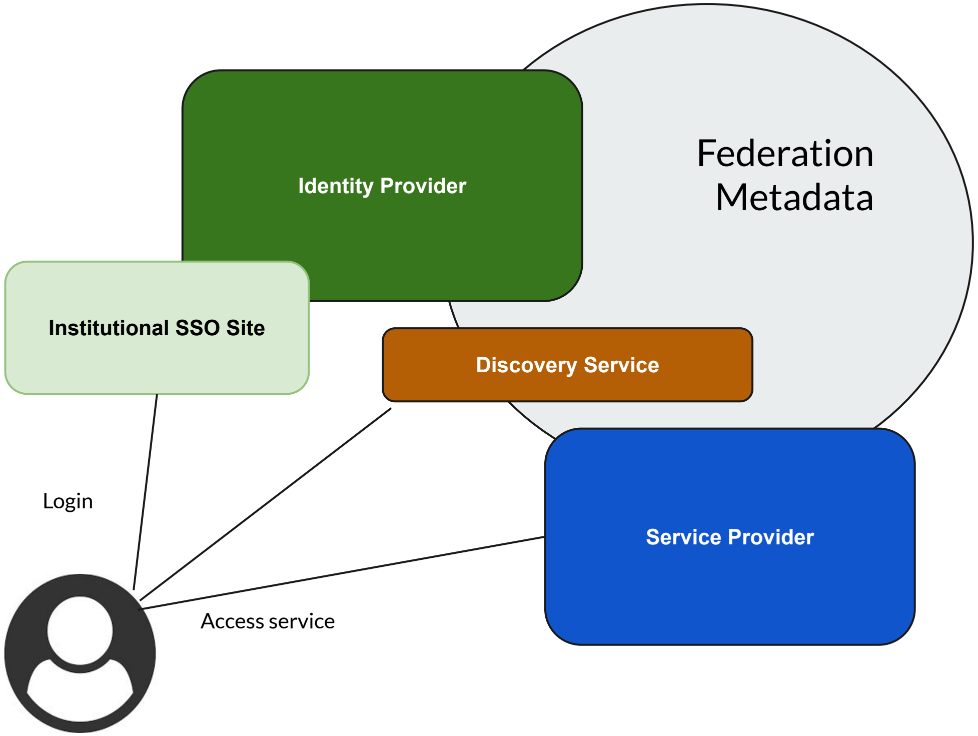


https://duo.com/blog/the-beer-drinkers-guide-to-saml

Authentication and Federation

Federation concepts

- Trust
- Metadata
- Entity Tagging
- Discovery Service
- Attribute Release Policies

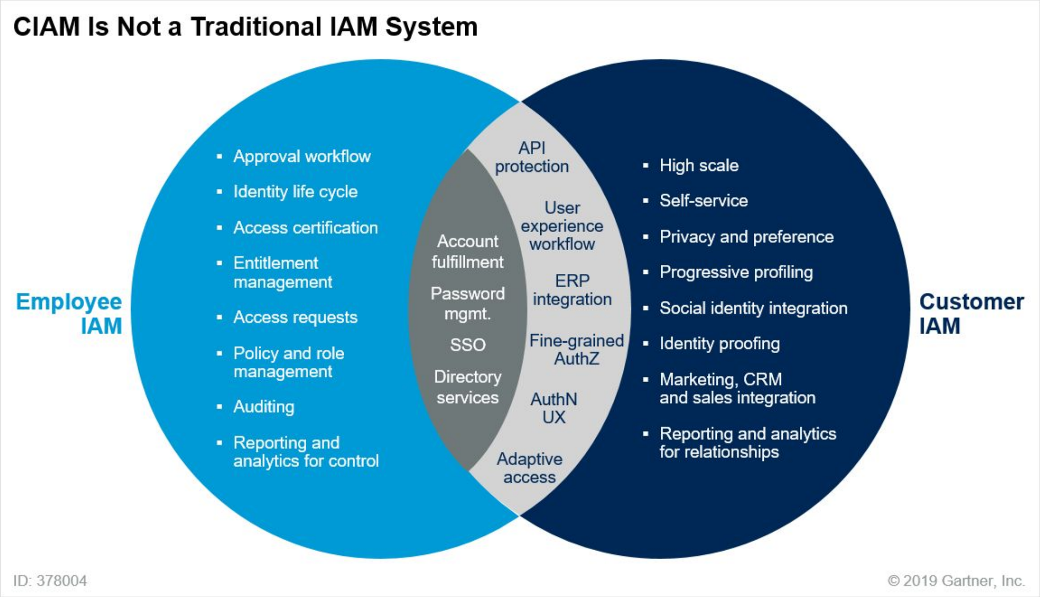


Implement Research and Scholarship Entity Category

Authentication and Federation

Futures

- CIAM - Consumer Identity and Access Management
  - Gartner - “Employee / Customer Convergence”
- Per-Entity Metadata (MDQ) - The Future is Today!
- IdPaas - IdP As A Service
- “Bring your own Identity” and Self-Sovereign Identity
- Citizen Identity (eIDAS, eduID)



Questions?

That was a lot to cover!

Please post questions in chat throughout the conference..

and THANK YOU!!