BCNET

Shared IT Services for Higher Education & Research

Conference 2017

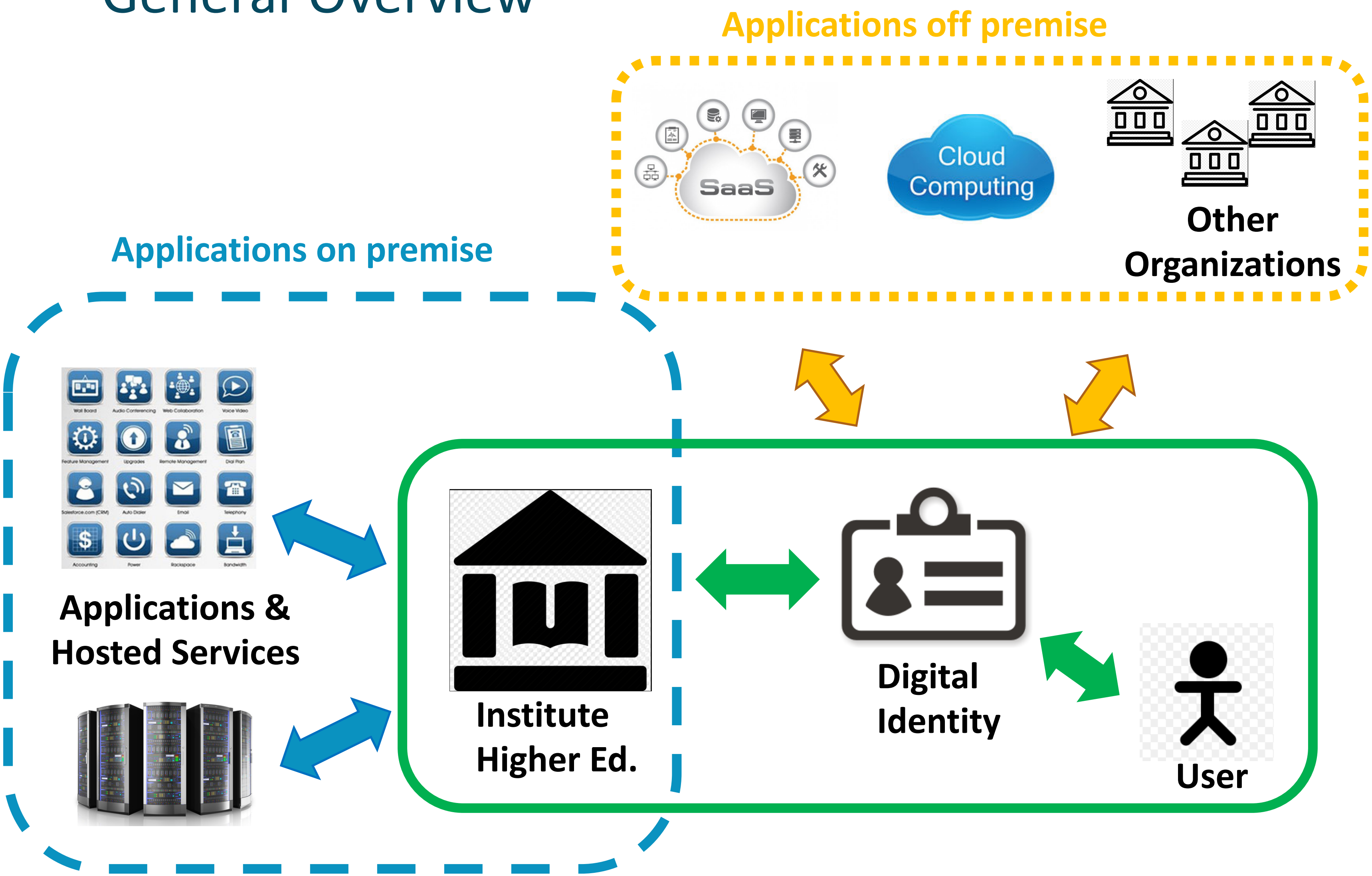
Identity Management and Service Integration in Higher Education

BCNet Identity Management Working Group

Speakers:

- Corey Scholefield | BCNet EduTrust, UVic
- Keir Novik | SFU
- Andy Zoltay | RRU
- Rahim Virani | KPU
- Sebastian Gonzalez | UBC
- Sabrina da Silva | BCIT

General Overview



Applications off premise

SaaS

Cloud Computing

Other Organizations

Applications on premise

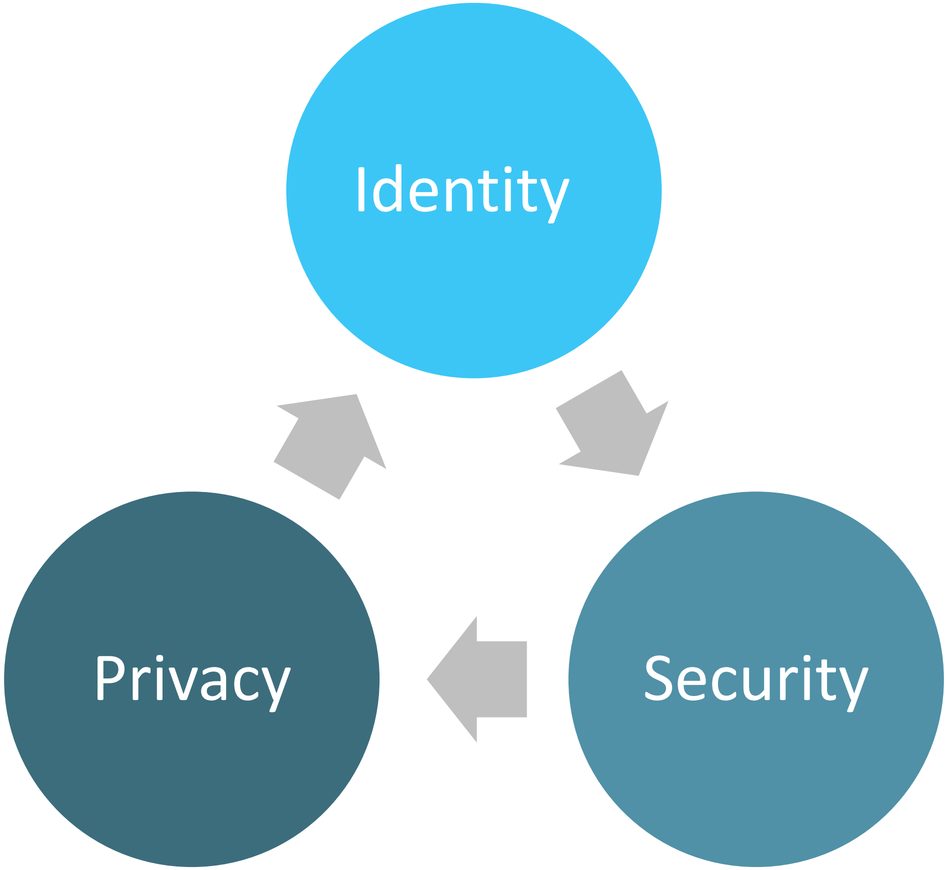
Applications & Hosted Services

Institute Higher Ed.

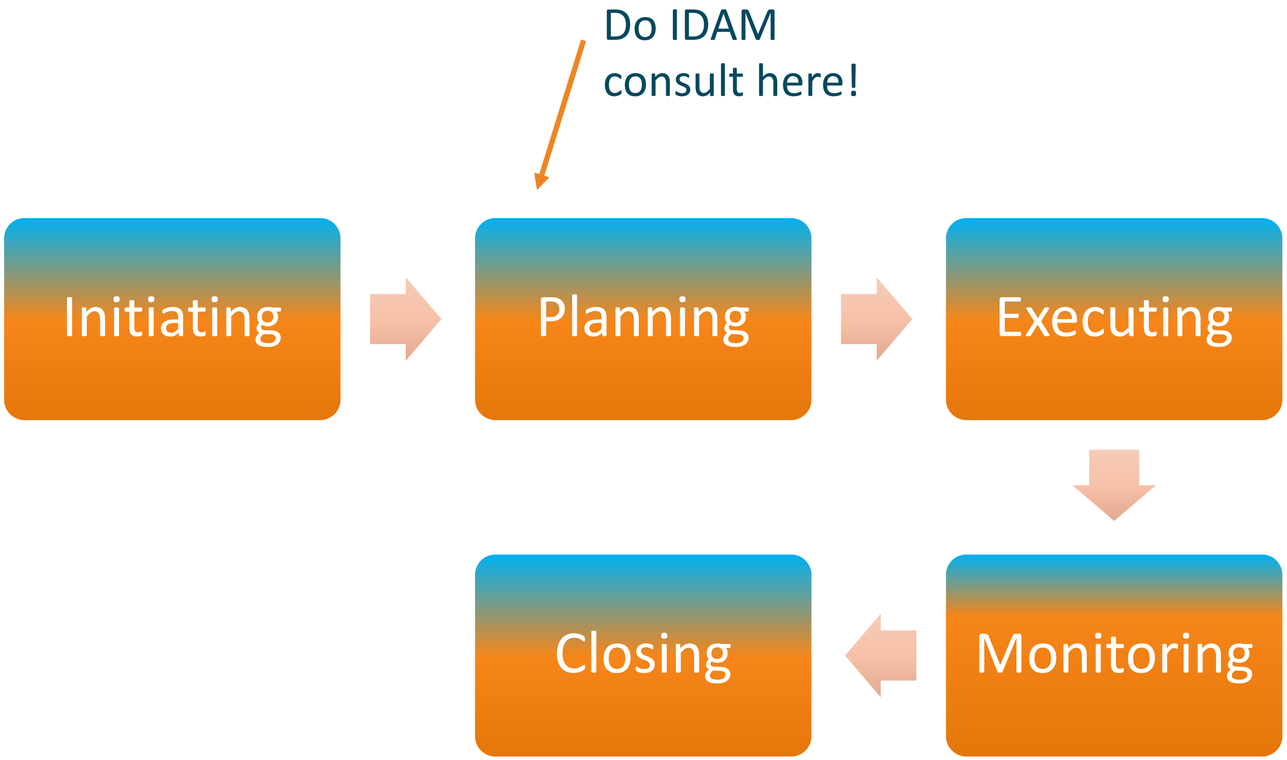
Digital Identity

User

Identity & Access - Planning Context



Identity and Access - Planning + Project Process


Do IDAM consult here!

Initiating

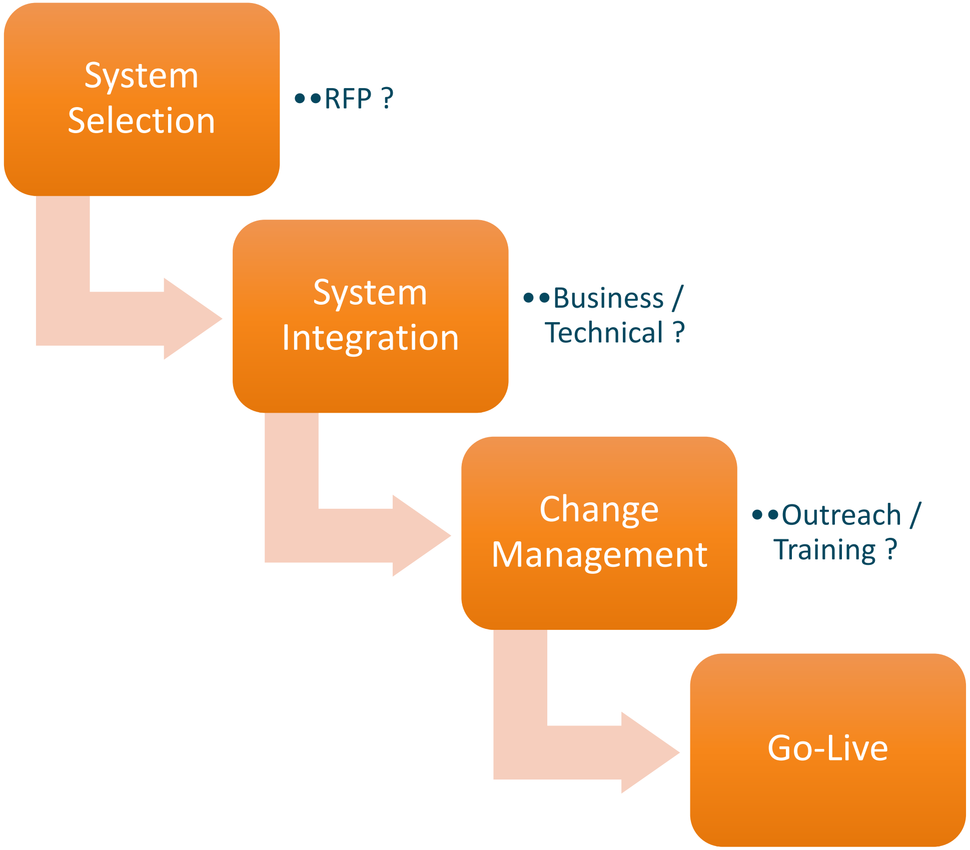
Planning

Executing

Monitoring

Closing

Services Integration Phases



System Selection

••RFP ?

System Integration

••Business / Technical ?

Change Management

••Outreach / Training ?

Go-Live

Identity and Access - Planning Alphabet

- autheNtication
- authoriZation
- accounts Provisioning
- accounts De-provisioning

*Thanks to Luca Filipozzi and Doug Gregg (UBC)

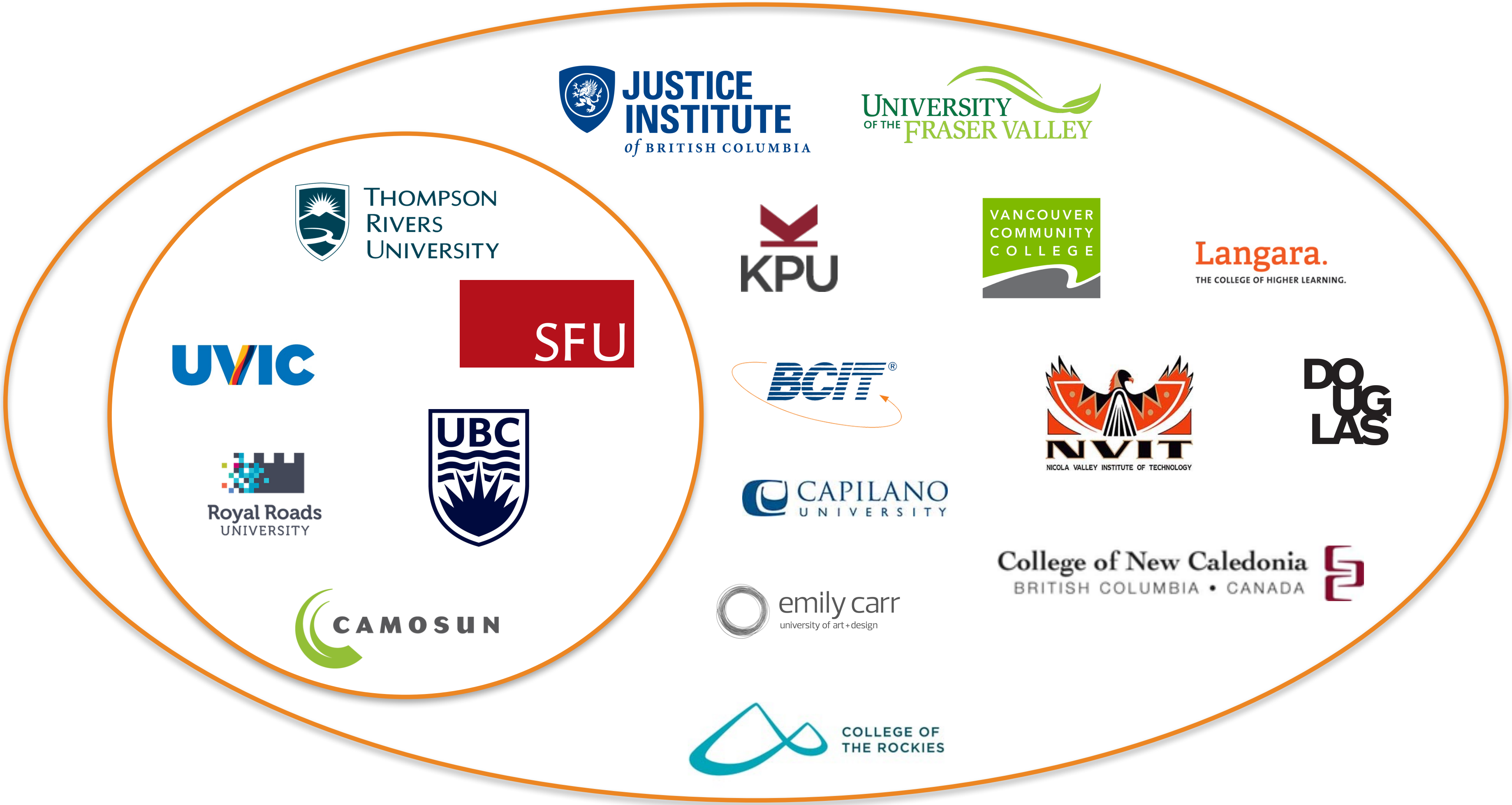
Identity and Access ‑ Planning Alphabet

- autheNtication
  - Campus options vs. system capability
- authoriZation
  - Permissions assignment – roles / groups / local vs. centralized
- accounts Provisioning
  - Business Process ? Just-in-case vs. Just-in-time ?
- accounts De-provisioning
  - Disable / timeline / retention / ongoing-access / grace-period ?

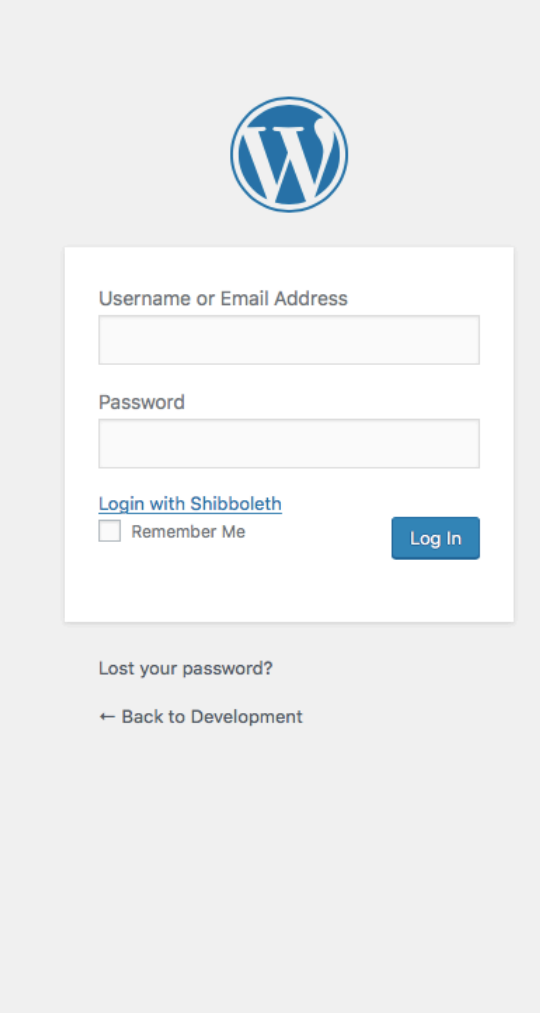
BC EduTrust Federated Services - Updates

- Goals
- every BCNET member:
  - runs eduroam WiFi service
  - runs federated SSO Identity Provider (IdP) in the Canadian Access Federation
  - support BCNET IT Shared Services adoption

BC EduTrust - CAF Community Group


JUSTICE INSTITUTE of BRITISH COLUMBIA
UNIVERSITY OF THE FRASER VALLEY
THOMPSON RIVERS UNIVERSITY
KPU
VANCOUVER COMMUNITY COLLEGE
Langara. THE COLLEGE OF HIGHER LEARNING.
SFU
UVIC
BCIT®
NVIT NICOLA VALLEY INSTITUTE OF TECHNOLOGY
DOUGLAS
UBC
Royal Roads UNIVERSITY
CAPILANO UNIVERSITY
College of New Caledonia BRITISH COLUMBIA • CANADA
emily carr university of art + design
CAMOSUN
COLLEGE OF THE ROCKIES

BC EduTrust / CAF / BCcampus ‐ Federated Wordpress



Username or Email Address

Password

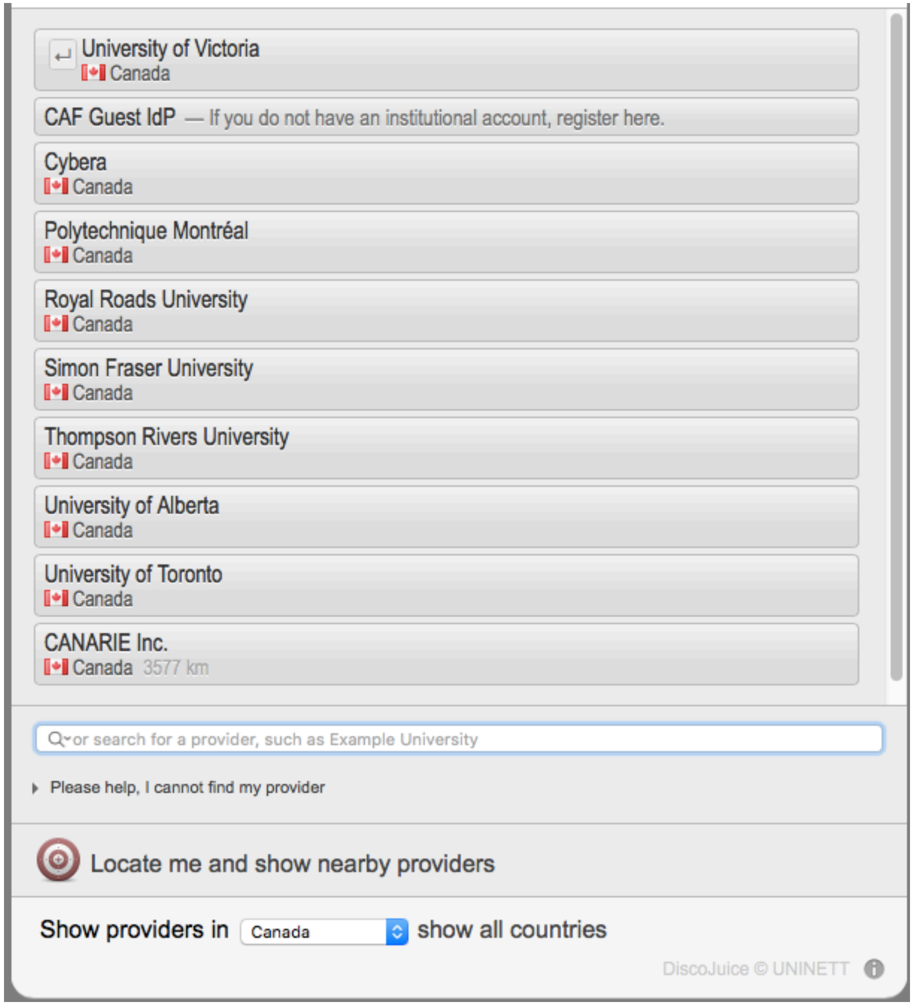
Login with Shibboleth

□ Remember Me

Log In

Lost your password?

← Back to Development



University of Victoria
Canada

CAF Guest IdP — If you do not have an institutional account, register here.

Cybera
Canada

Polytechnique Montréal
Canada

Royal Roads University
Canada

Simon Fraser University
Canada

Thompson Rivers University
Canada

University of Alberta
Canada

University of Toronto
Canada

CANARIE Inc.
Canada 3577 km

or search for a provider, such as Example University

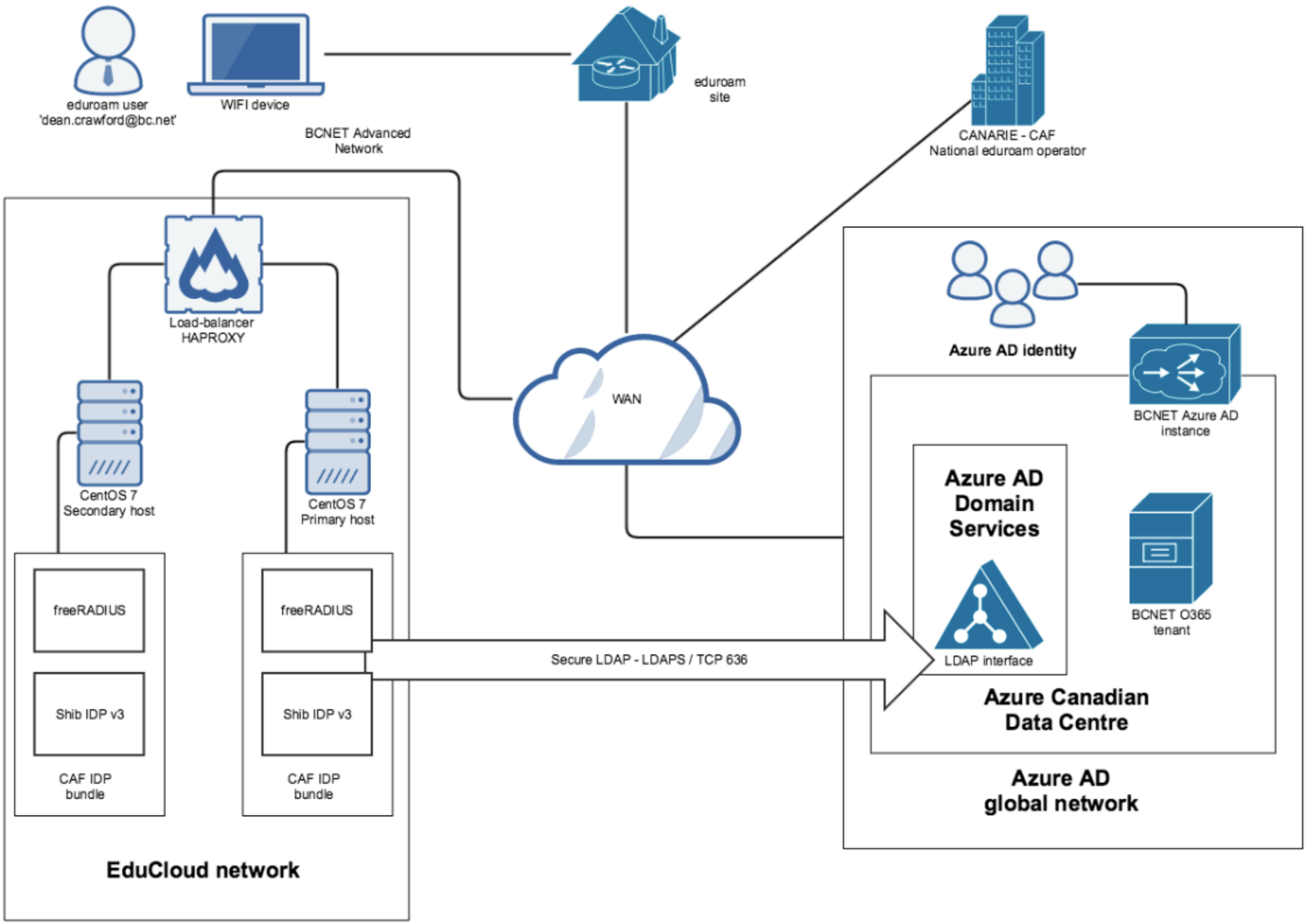
Please help, I cannot find my provider

Locate me and show nearby providers

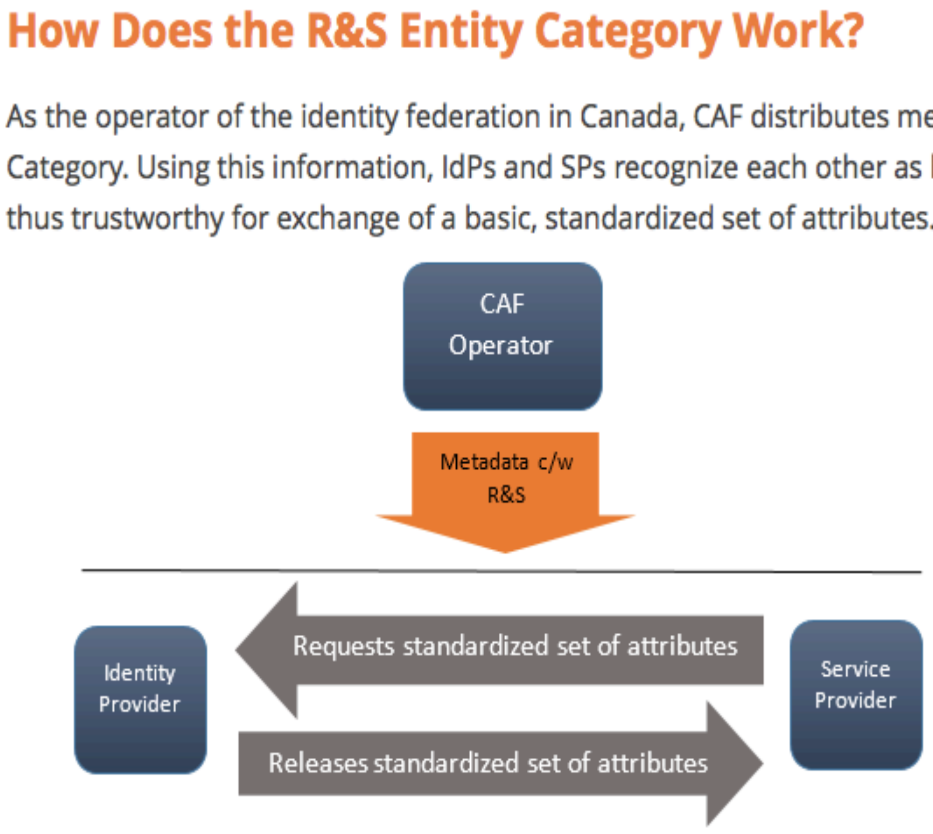
Show providers in Canada show all countries

DiscoJuice © UNINETT

BC EduTrust ‑ eduroam for @bc.net accounts on Azure AD



BC EduTrust - CAF Research & Scholarship Entity Category Support



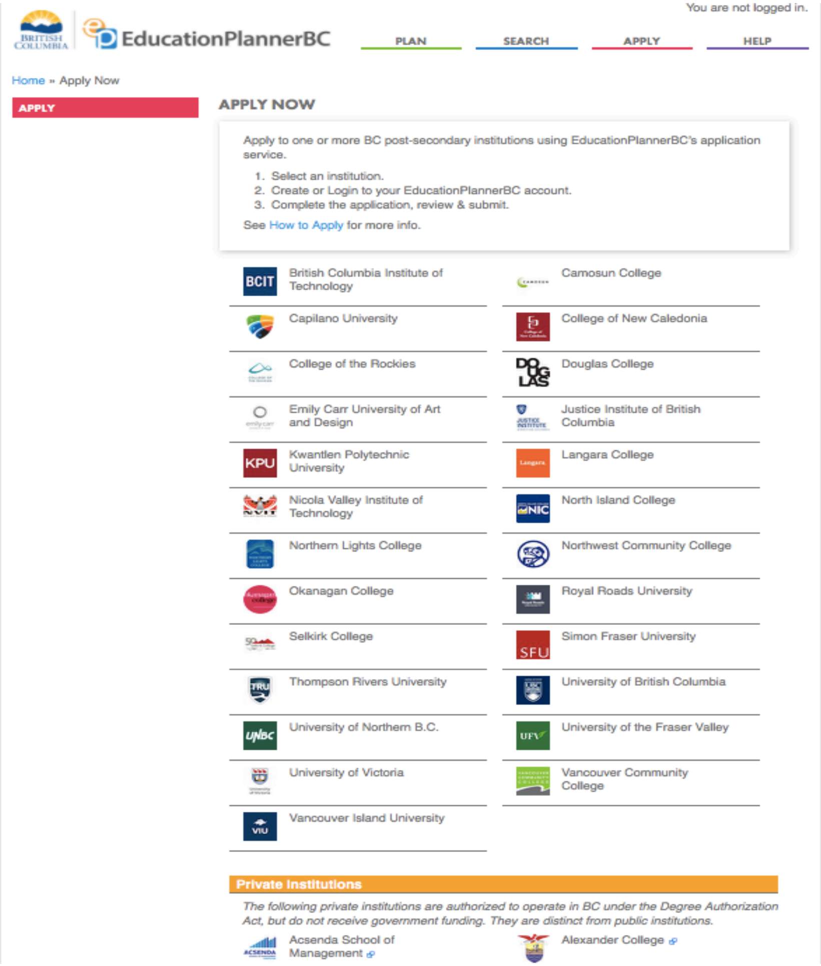
How Does the R&S Entity Category Work?

As the operator of the identity federation in Canada, CAF distributes metadata indicating which entities support the R&S Entity Category. Using this information, IdPs and SPs recognize each other as being part of the research and education community and as thus trustworthy for exchange of a basic, standardized set of attributes.

CAF Operator
Metadata c/w R&S
Identity Provider
Requests standardized set of attributes
Releases standardized set of attributes
Service Provider

https://www.canarie.ca/identity/support/research-and-scholarship-entity-category/

BC EduTrust ‑ Education Planner (phase 3)



You are not logged in.

Home » Apply Now

APPLY

APPLY NOW

Apply to one or more BC post-secondary institutions using EducationPlannerBC's application service.

1. Select an institution.
2. Create or Login to your EducationPlannerBC account.
3. Complete the application, review & submit.

See How to Apply for more info.

- British Columbia Institute of Technology
- Camosun College
- Capilano University
- College of New Caledonia
- College of the Rockies
- Douglas College
- Emily Carr University of Art and Design
- Justice Institute of British Columbia
- Kwantlen Polytechnic University
- Langara College
- Nicola Valley Institute of Technology
- North Island College
- Northern Lights College
- Northwest Community College
- Okanagan College
- Royal Roads University
- Selkirk College
- Simon Fraser University
- Thompson Rivers University
- University of British Columbia
- University of Northern B.C.
- University of the Fraser Valley
- University of Victoria
- Vancouver Community College
- Vancouver Island University

Private Institutions

The following private institutions are authorized to operate in BC under the Degree Authorization Act, but do not receive government funding. They are distinct from public institutions.

- Acsenda School of Management
- Alexander College

Royal Roads University

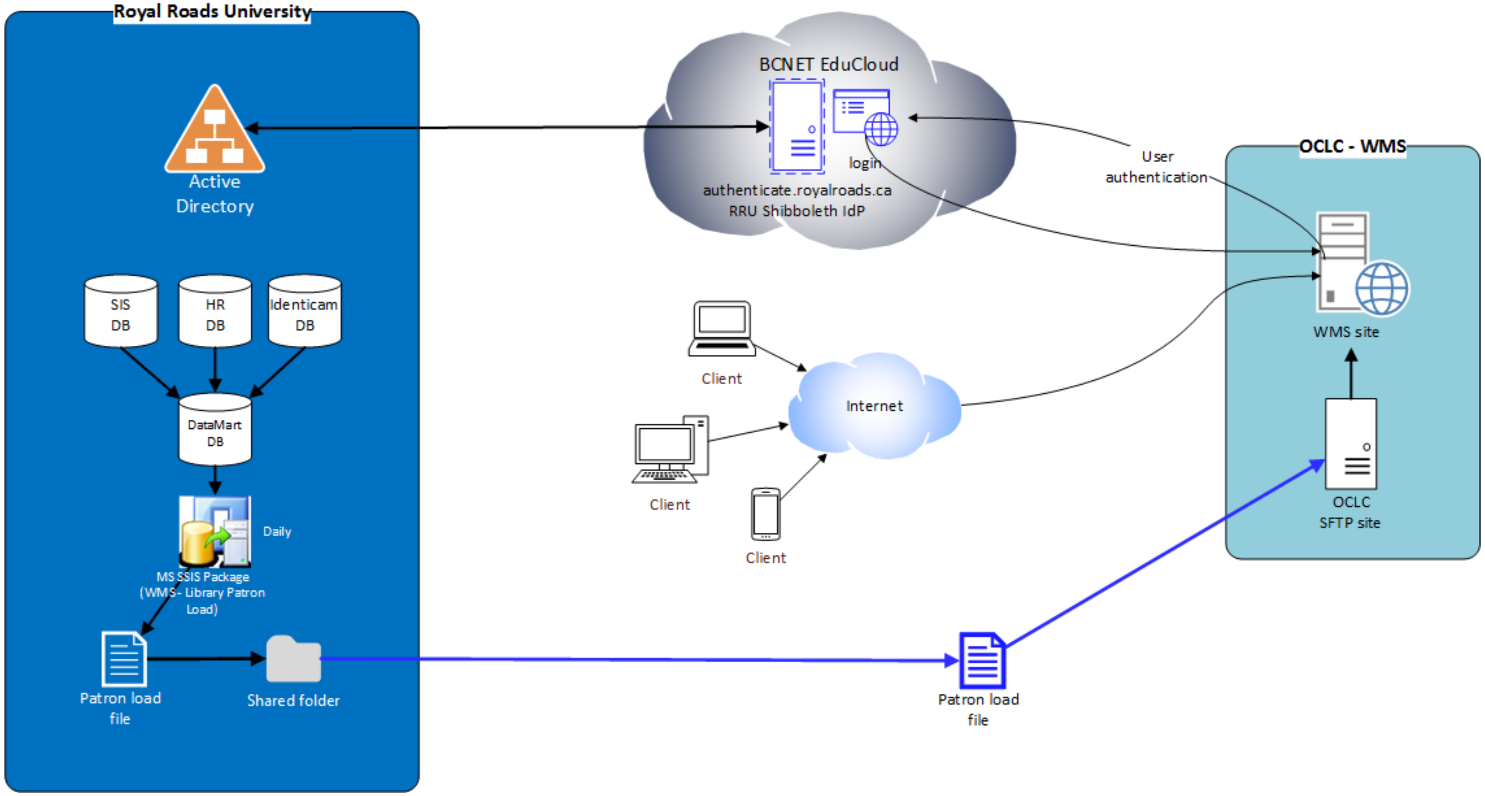
- Strategies
  - Consolidating identities into a single repository with multiple roles
  - Move towards central authentication
  - Streamlining account provisioning synchronization
- Challenges
  - Shibboleth is complicated and has a steep learning curve
  - Each service provider implementation has proven slightly different or non-standard
    - e.g. use of the “unspecified” format
    - e.g. Shibboleth vs ADFS
  - Shibboleth versioning differences has caused challenges
    - i.e. Version 3 of IdP and version 2 of SP

Royal Roads University

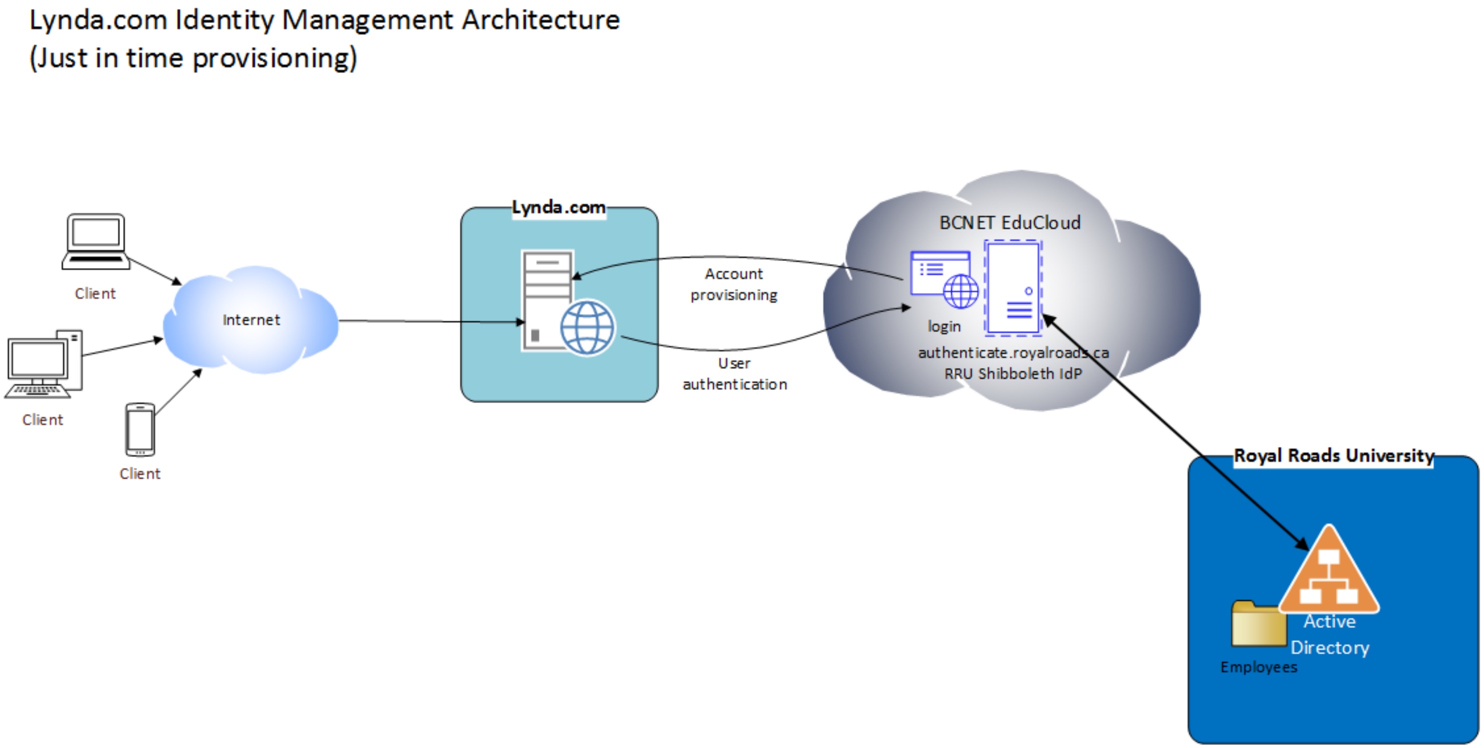
- Newly on-boarded off-premise services:
  - WorldShare Management Services (Library system)
  - WebSpace (WPCloud)
  - Lynda.com
  - HRSmart

Royal Roads University

WMS Identity Mangement Architecture
(Just in case account provisioning)



Royal Roads University



Lynda.com Identity Management Architecture
(Just in time provisioning)

Andy Zoltay
2017-04-20

IDAM - KPU strategies

- User Experience (UX) driven
- Minimize security footprint
- IaaS and SaaS (“Cloud-enabled”)

IDAM Struggles

- Exceptions to calculated roles and definitions (vendors, visiting scholars, recruiters etc.)
- Single identity, multiple role vs. multiple identity, multiple role service mapping
- Creative account access workflows
- Federated Identity knowledge barrier of entry
- Some applications just don't support Single/SameSignon

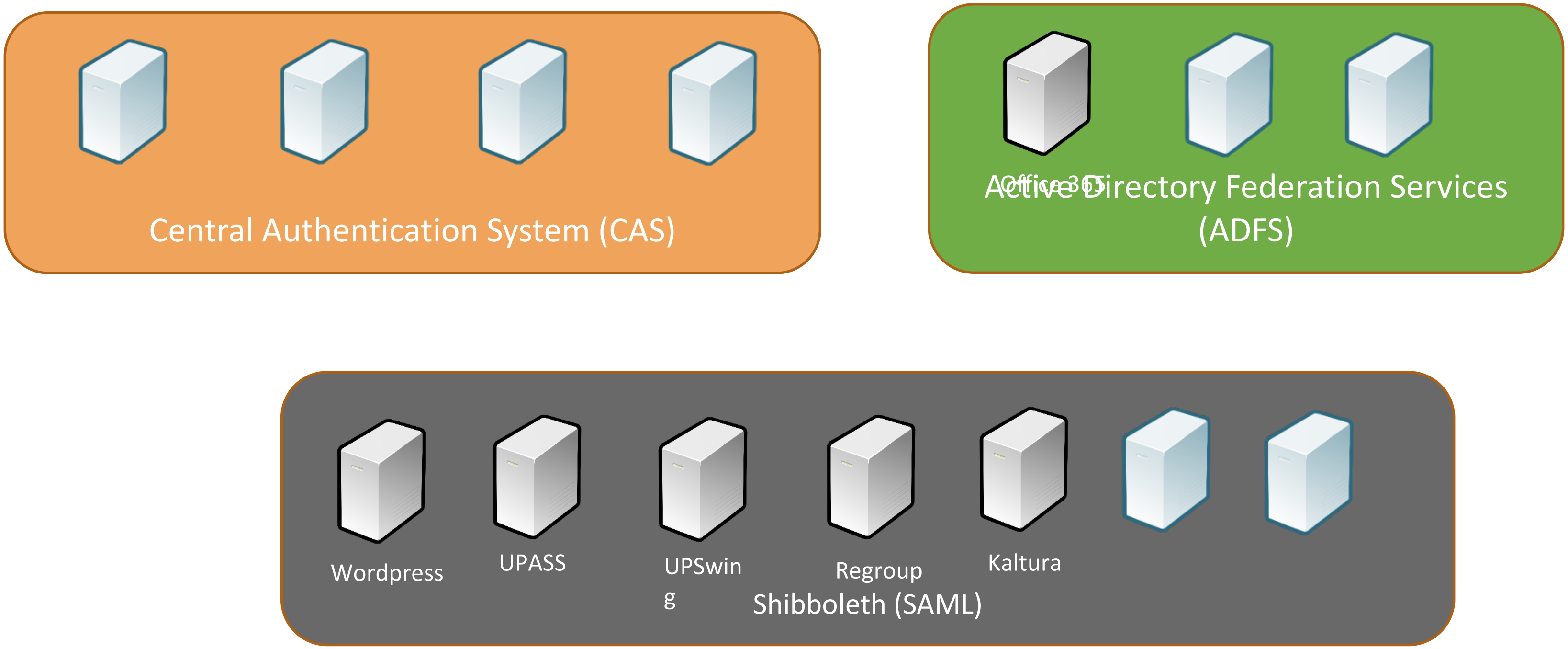
IDAM Accomplishments

- Simple architecture, no heavy ETL and staging processes as well as data processing overhead.

- Future ready:
  - Directory Consolidation
  - SSO onboarding
  - Banner XE

- In process of onboarding most popular candidates to SSO (Self-Service, Learning Management System, Navigation Portal, SharePoint, Office 365 etc..)*

Current State



Central Authentication System (CAS)

Office 365

Active Directory Federation Services (ADFS)

Wordpress

UPASS

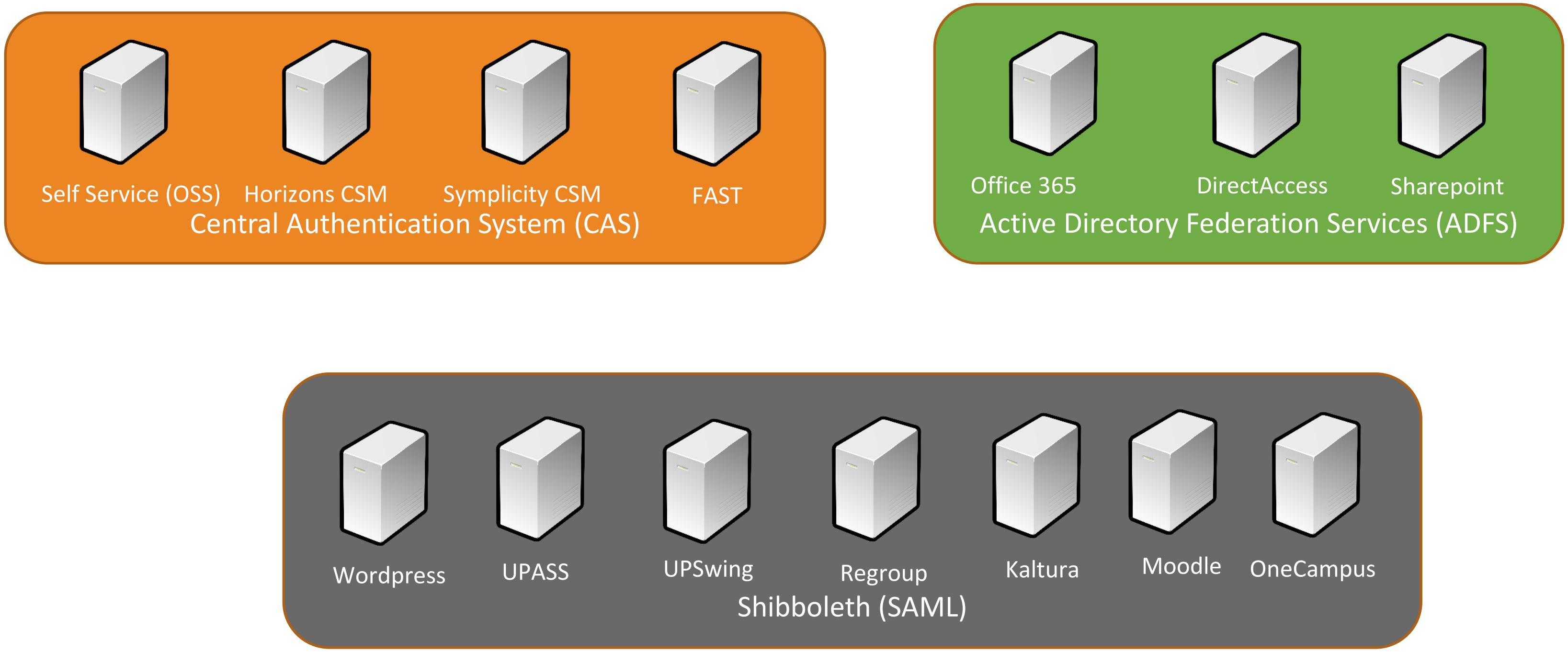
UPSwin
g

Regroup

Kaltura

Shibboleth (SAML)

Future State



Self Service (OSS) Horizons CSM Symplicity CSM FAST

Central Authentication System (CAS)

Office 365 DirectAccess Sharepoint

Active Directory Federation Services (ADFS)

Wordpress UPASS UPSwing Regroup Kaltura Moodle OneCampus

Shibboleth (SAML)

High Level Metrics - KPU

Total Applications	60
Total Applications Off Premise	25%
Supporting SSO (Single and Same SignOn)	50%
Single SignOn Implemented	10%
Same SignOn Implemented	80%

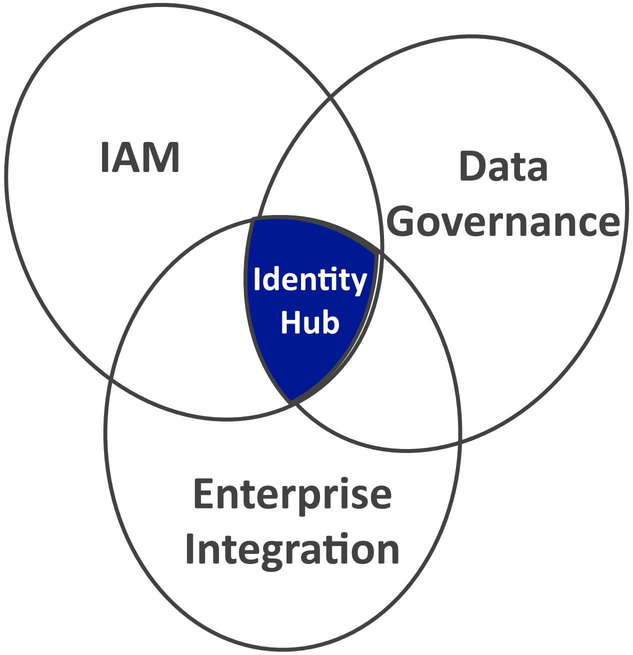
Simon Fraser University

- Strategies
  - Be principally a provider of cloud services
  - Use cloud services with maximum value while minimizing risk
  - Single sign-on through CAS
  - Federated identity through CAF
- Struggles
  - Preserving privacy
  - Value proposition of IDAM
- Accomplishments
  - Compute Canada ARC site at SFU
  - SFU Vault

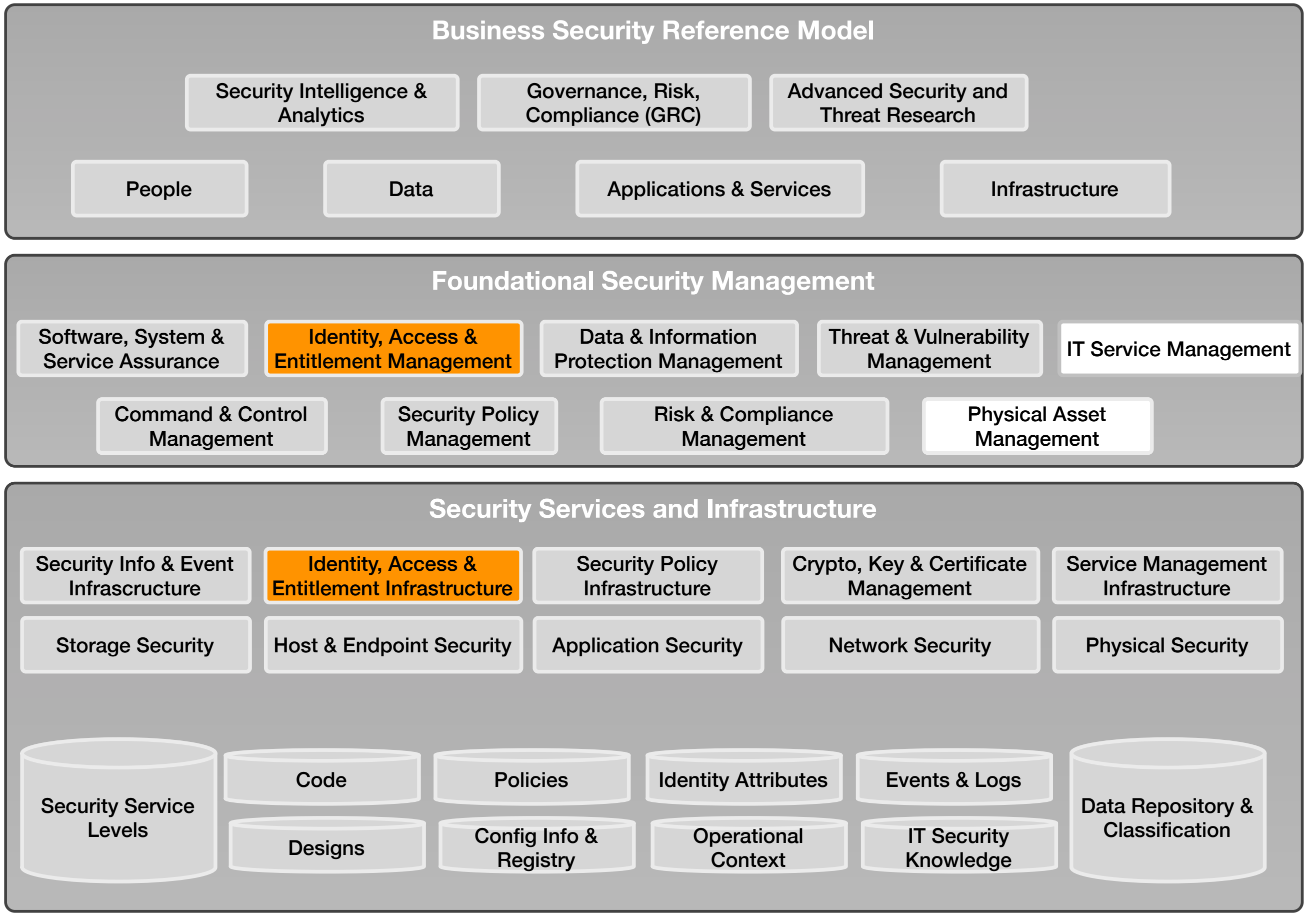
UBC

- IAM as an integrator for ERP renewal (Cloud Landscape)
- IAM Realignment
  - Office of CIO under the CISO portfolio
- Transitioning form a Infrastructure Dept. with a Security component to a Security Discipline with Infrastructure Responsibilities.
- Heavy lifting into the cloud.

IAM as an integrator for ERP renewal (Changing Cloud Landscape)



IAM Realignment



Business Security Reference Model

Security Intelligence & Analytics

Governance, Risk, Compliance (GRC)

Advanced Security and Threat Research

People

Data

Applications & Services

Infrastructure

Foundational Security Management

Software, System & Service Assurance

Identity, Access & Entitlement Management

Data & Information Protection Management

Threat & Vulnerability Management

IT Service Management

Command & Control Management

Security Policy Management

Risk & Compliance Management

Physical Asset Management

Security Services and Infrastructure

Security Info & Event Infrascructure

Identity, Access & Entitlement Infrastructure

Security Policy Infrastructure

Crypto, Key & Certificate Management

Service Management Infrastructure

Storage Security

Host & Endpoint Security

Application Security

Network Security

Physical Security

Security Service Levels

Code

Designs

Policies

Config Info & Registry

Identity Attributes

Operational Context

Events & Logs

IT Security Knowledge

Data Repository & Classification

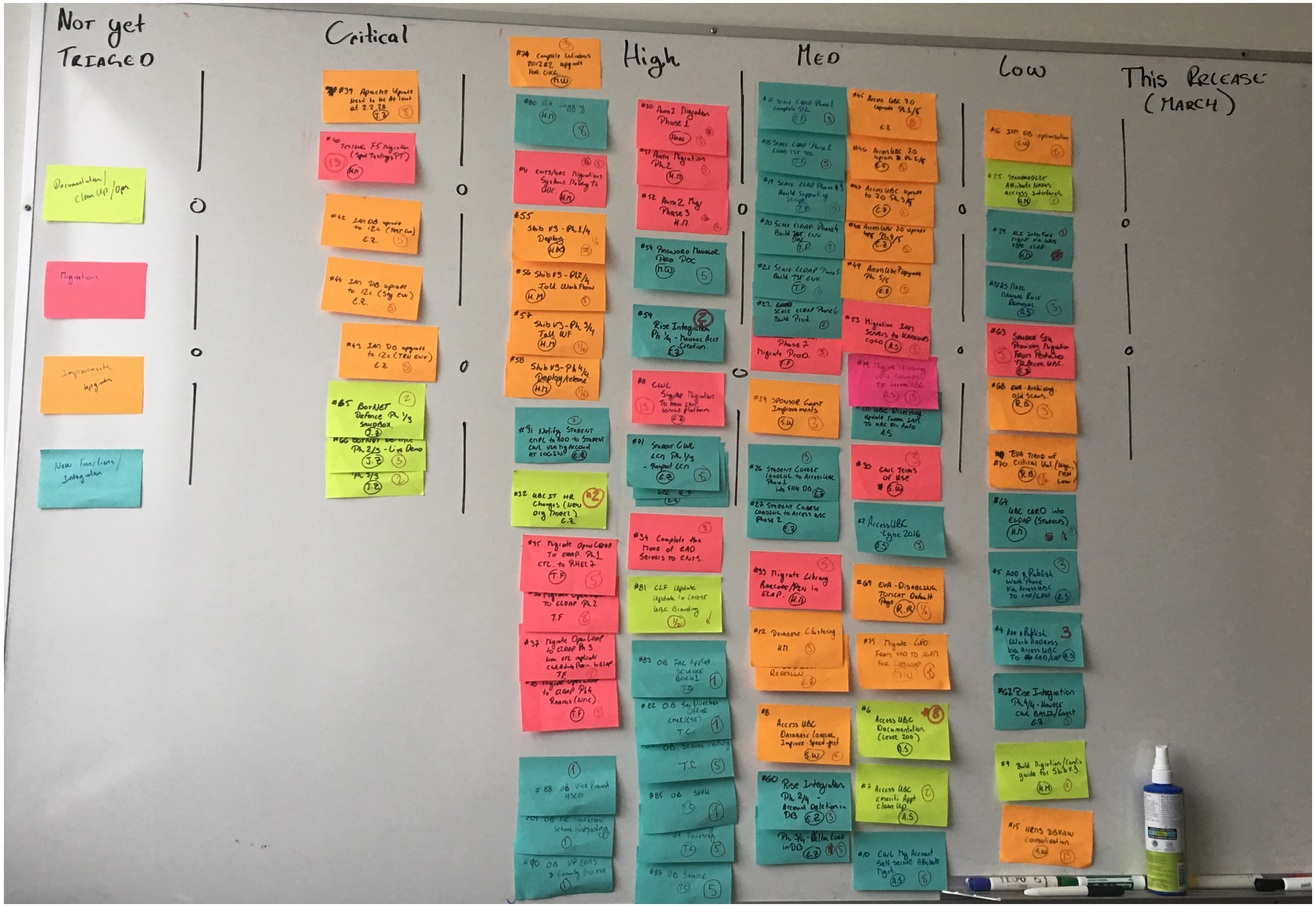
Transitioning form a Infrastructure Dept. with a Security component to a Security Discipline with Infrastructure Responsibilities.

Drastically reduce attack surface

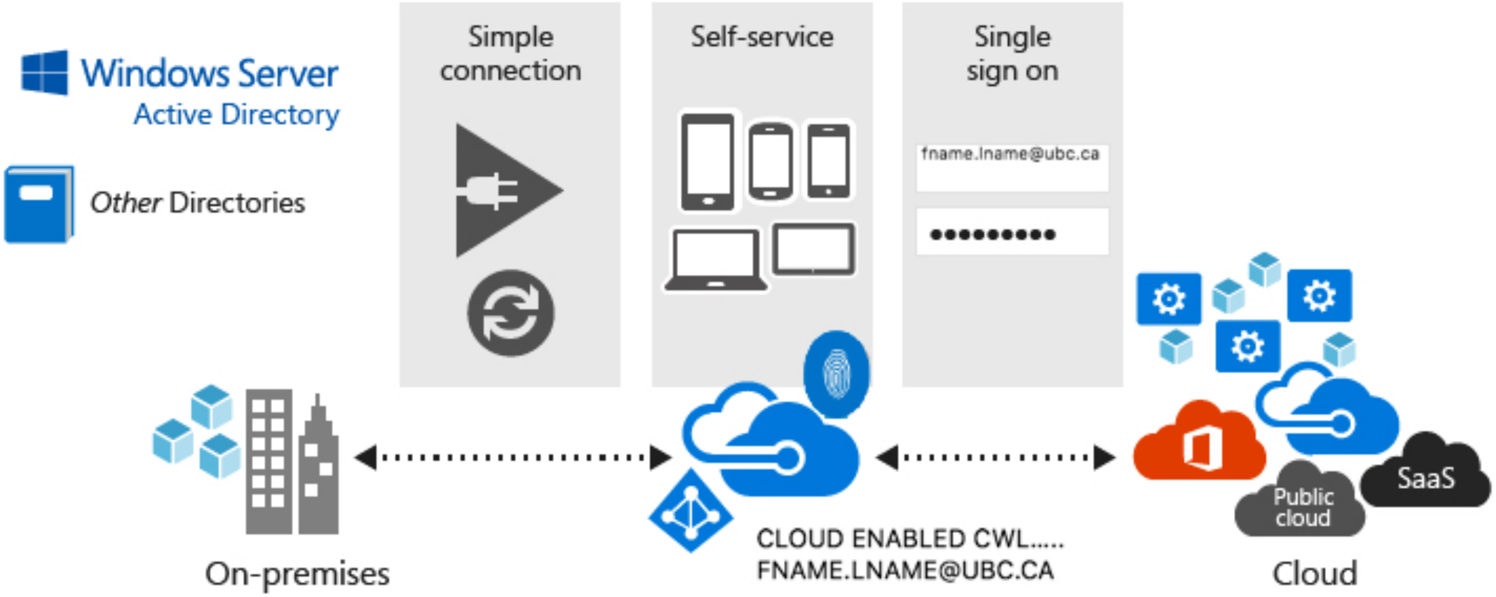
Strengthen Controls

Increase Analytics Capabilities

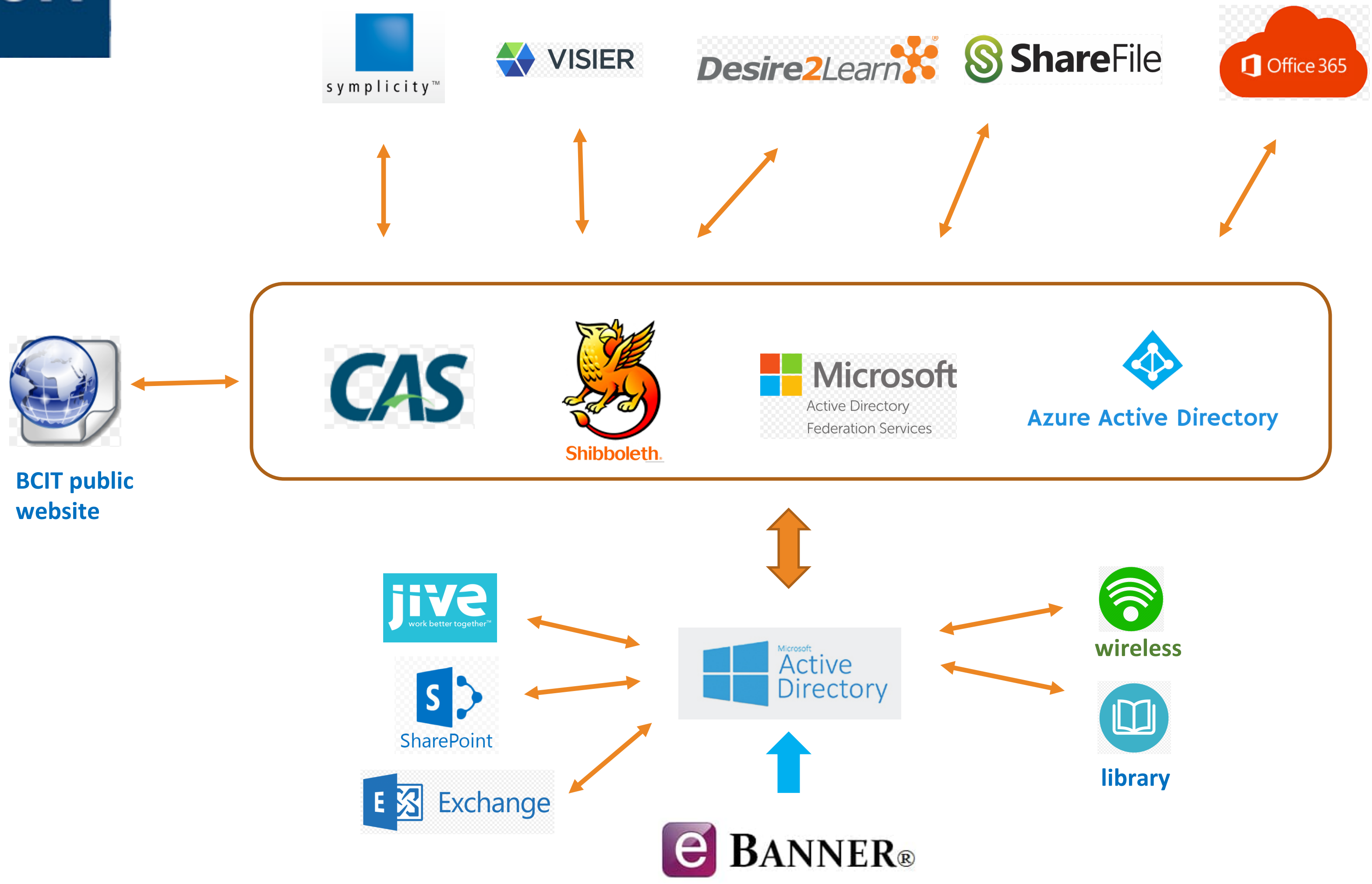
Payment Plan on "Technical Debt"



Heavy lifting into the cloud



Integration of Services and Applications



symplicity™

VISIER

Desire2Learn

ShareFile

Office 365

BCIT public website

CAS

Shibboleth.

Microsoft Active Directory Federation Services

Azure Active Directory

jive work better together™

SharePoint

Exchange

Microsoft Active Directory

BANNER®

wireless

library

Integration of Services and Applications

- Strategies
  - Enhance user experience
  - Simplification and optimization of services
- Struggles:
  - Preserving privacy
  - IDAM road map
- Accomplishments
  - Onboarding new services
  - Consolidating services

Questions