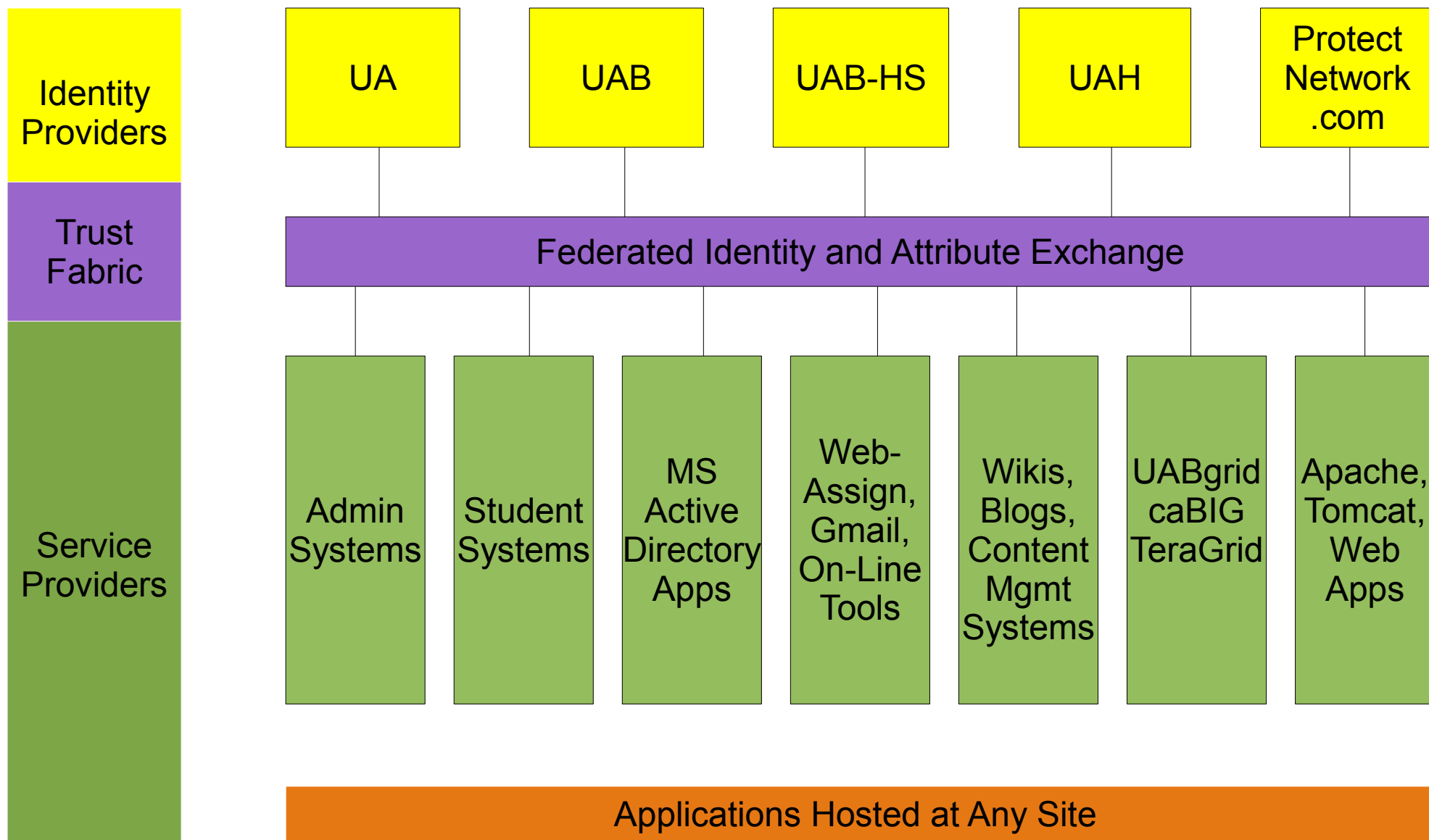


# Federated Identity and Access Management for the University of Alabama System

John-Paul Robinson <[jpr@uab.edu](mailto:jpr@uab.edu)>  
Infrastructure Services  
UAB IT

# Consistent Identity and Access Management (IAM) Simplifies Service Creation

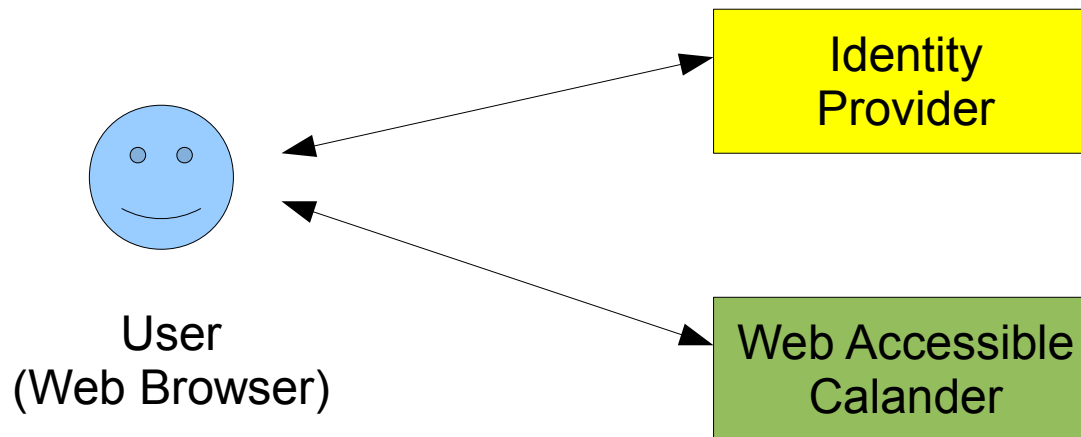


# Project Impacts at UAB

- Federated “Global” Directory
  - Basic User Profile: Identity, Affiliation, Email
  - Custom User Profiles on Per-Application Basis
  - Microsoft Active Directory Supports Federation
  - BlazerNet and SharePoint Access
- SoM “UABgrid” RFA
- UAB HPC Expansion (TeraGrid, OSG, SURAGrid)
- Optionally Supply Select Attributes to Non-UAB Entities
  - caBIG
  - NIH
  - TeraGrid, National Cyberinfrastructure
  - WebAssign

# An Example Application

- Controlled Access to Calendars
  - User Requests Calendar Access
  - Campus Asserts User Identity and Attributes
  - Calendar Application Restricts Access to Select Users with appropriate roles
  - Calendar Entries Available to User and Client Tools



# History of Development

- **2003:** UAB Oracle system integrated with BlazerID system (without password replication)
- **2003-2006:** UAB IT, UAB CIS, Internet2, NCSA collaborate on NSF funded project to develop integrated web and non-web authorization system called myVocs, which leverages Shibboleth and GridShib. Developed OpenIdP.org to facilitate use by non-Shibboleth sites.
- **2007-2008:** myVocs authorization system leveraged as core of UABgrid collaboration environment. myVocs model adopted by the CoManage Internet2 project, similar architecture adopted by other grids (e.g. D-Grid). **UABgrid Pilot deployed to demonstrate benefits to applications of consistent interface across “internal” and “external” infrastructure.**
- **2009:** Taking the next steps...

# Case Studies & References

- UK Schools
- Library Resource Access
  - New Internet Pilot Starting: <https://spaces.internet2.edu/display/inclibrary/InC-Library>
- Microsoft [DreamSpark](#) – MS Development tool download for students
- [ProtectNetwork.com](#) – a commercial identity provider that provides identity verification for individuals and identity implementation services for organizations.
- InCommon Federation site with additional Case Studies:  
<http://www.incommonfederation.org>
- Integrating Microsoft Active Directory Federation Services and Shibboleth
  - “[Scenario 2](#)” describes the Shibboleth Identity Provider and MS ADFS client configuration.
- [myVocs.org](#) – provides a VM with integrated group management and collaboration tools
- [OpenIdP.org](#) – provides identity services to non-Shibboleth user
- “[Campus Middleware in the Service of Scientific and Scholarly Workflow](#) ” by Keith Hazelton, University of Wisconsin
- “[A Concept for Attribute-Based Authorization on D-Grid Resources](#) ” Groeper, R. et. al.