Identity Management

...

A Tale of Two Auths

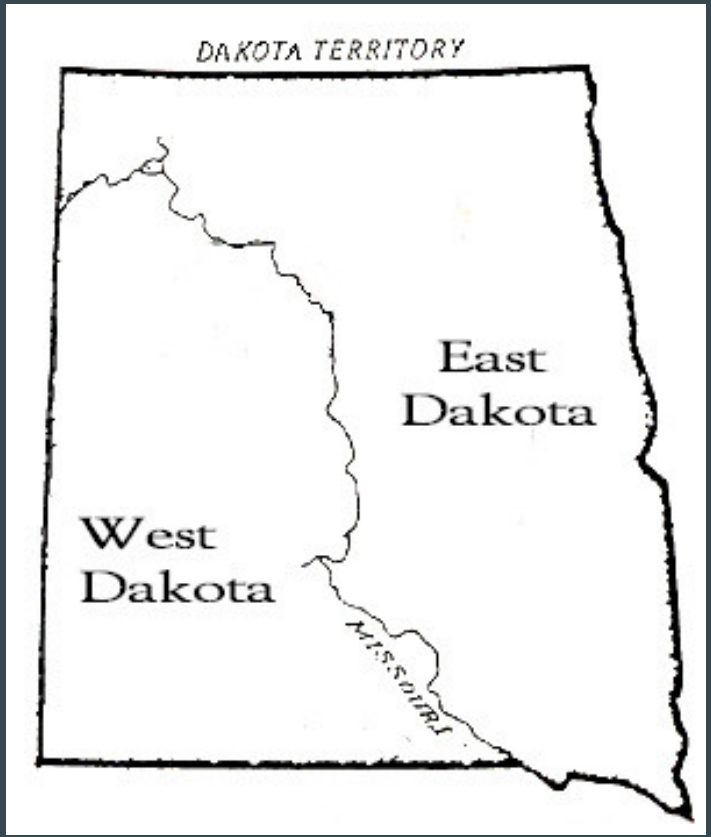
Managing Identities is Managing Data

Specifically IDM uses and stores data related to two central tasks

- Authentication (authn) - Knowing that someone is who they say they are
- Authorization (authz) - Knowing what that person has access to do

History of IDM at East Dakota U

What follows is a fictional but plausible account of how authn, authz and IDM evolved at East Dakota U, or EDU.edu.



The Mainframe Days

In the early 70s, E.D. U invested in its first mainframe, lovingly called The Mainframe

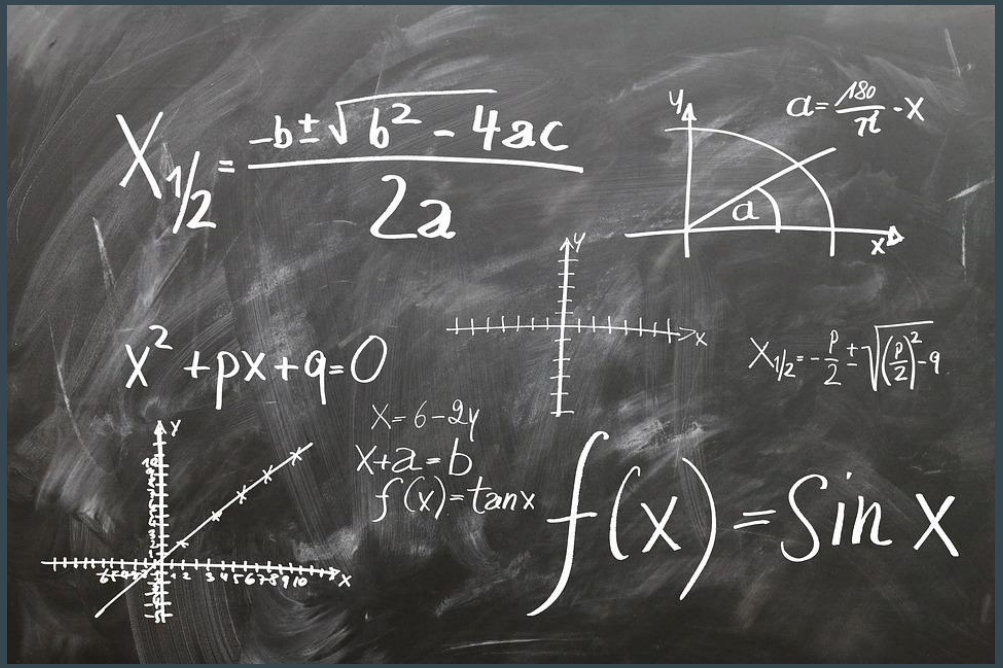
Identities were stored on The Mainframe

All authn and authz tasks were performed on The Mainframe

IDM was easy

Multiple Systems, Multiple Identities

- By the early 80s mainframes became both cheap enough and useful enough that departments around campus started buying their own
- These systems were not interconnected
- Users had different credentials on each system



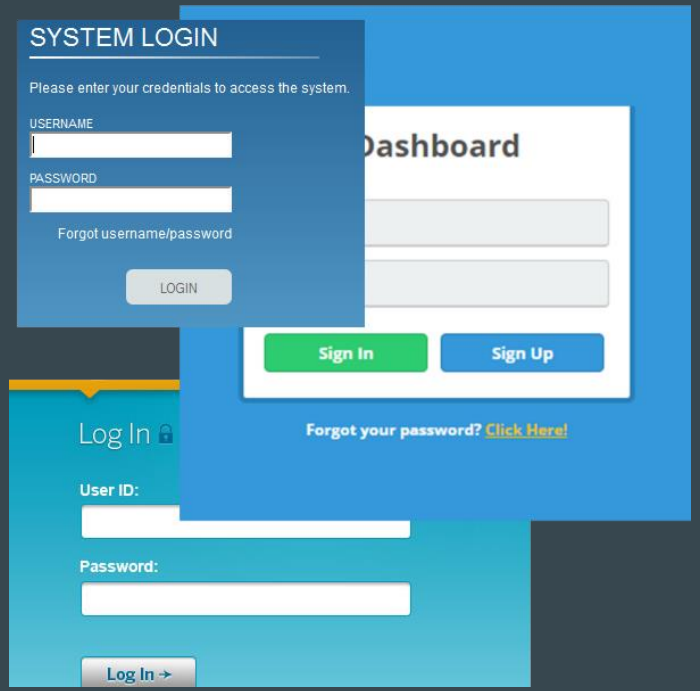
Central IDM Database, Many Applications

In the 90s mainframes gave way to web servers

Credentials were consolidated into a central database

Applications would require a user's credentials and connect to the DB to authenticate

Authorization decisions were left up to the applications

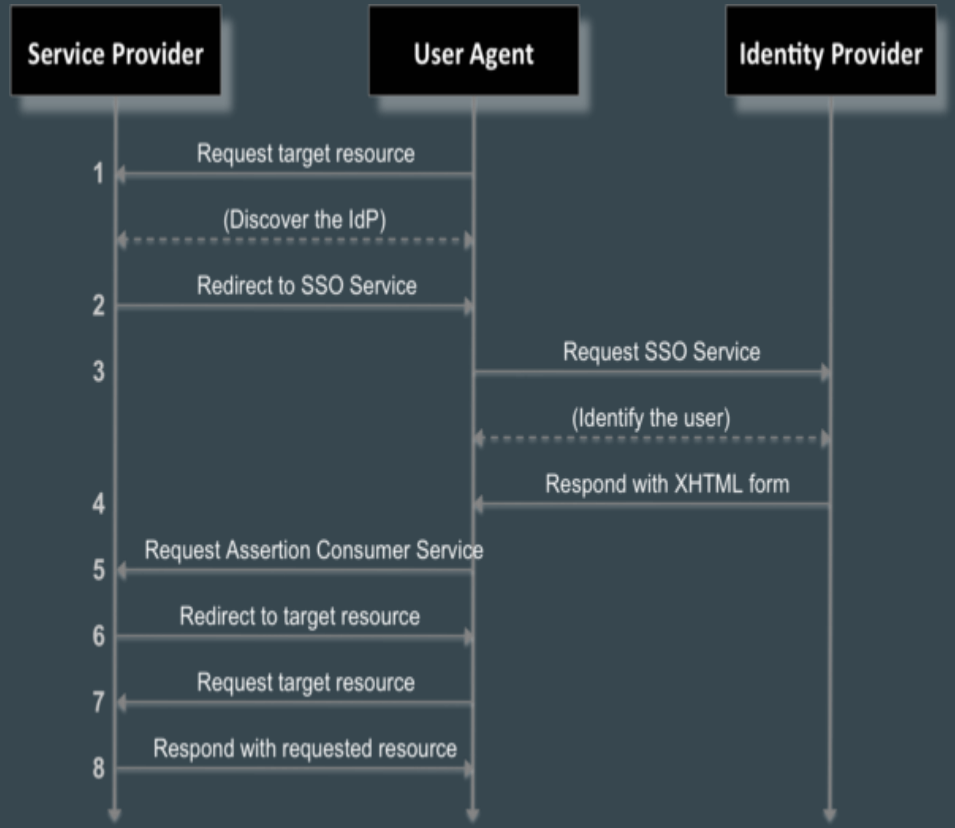


Centralized Authn with Provisioning

- Move all authentication to a central login page
- Allows for Single Sign On (SSO)
- Generates a cryptographically signed cookie visible to entire edu.edu domain
- Does not address authorization concerns
- Does not work for sites outside of the edu.edu domain

Centralized Authn with Attribute Release

- In the early 2000's the first RFCs for the Security Assertion Markup Language (SAML) were proposed
- Open standard data format for exchanging authn and authz data between parties
- IDM capabilities reside inside Identity Providers (IdPs)
- Services that rely on IdPs for authn



Shibboleth, InCommon, and Internet2

- Shibboleth is like a dialect of SAML
- Shibboleth is also a set of programs that support the shibboleth dialect (IdPs and SPs)
- Apache 2 Open Source License
- Trust between domains is accomplished using public/private key cryptography

Shibboleth®

InCommon®

INTERNET®2

Federations

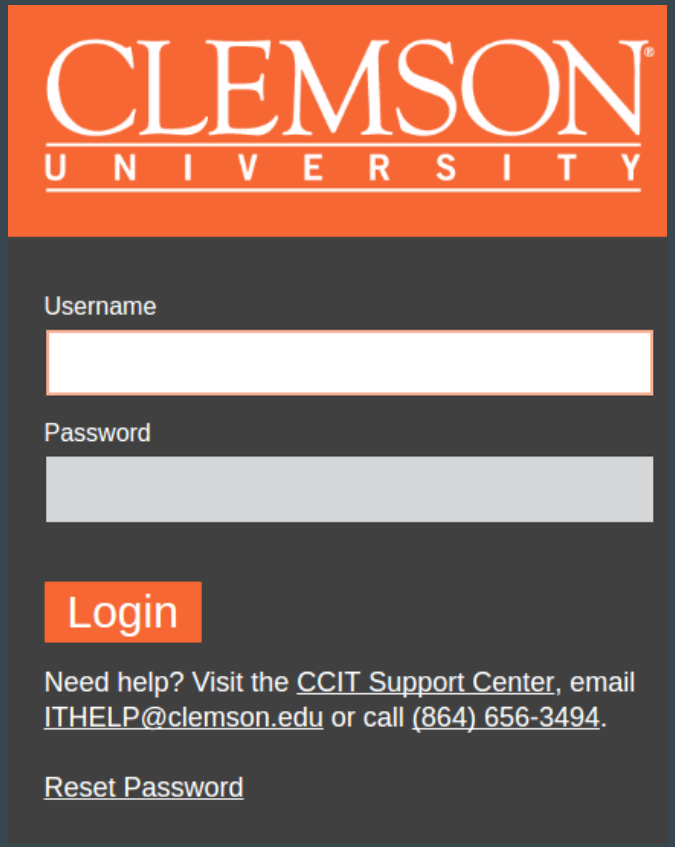
- Federations aggregate the necessary metadata and keys and produce a single consumable xml document
- Where Are You From (WAYF) pages
- InCommon for Higher Ed in the US
- eduGain: a federation of federations

InCommon® FEDERATION

eduGAIN

Shibboleth at Clemson

- IdP consists of 4 web servers in Layer 7 load balanced cluster
- Apache -> tomcat 8 -> idp.war
- War file built from resources stored in SVN
- Salt and salt-cloud managed
- SPs are installed and configured upon request
- Normal SP configuration requests



Thank you!
Questions?

Craig Baker
cbaker@clemson.edu
openclemson.ghost.io