Take No Pretenders: Identity and Access Management

ITS Webinar
10/7/2014

Eric Goodman, IAM Architect

Webinar Overview

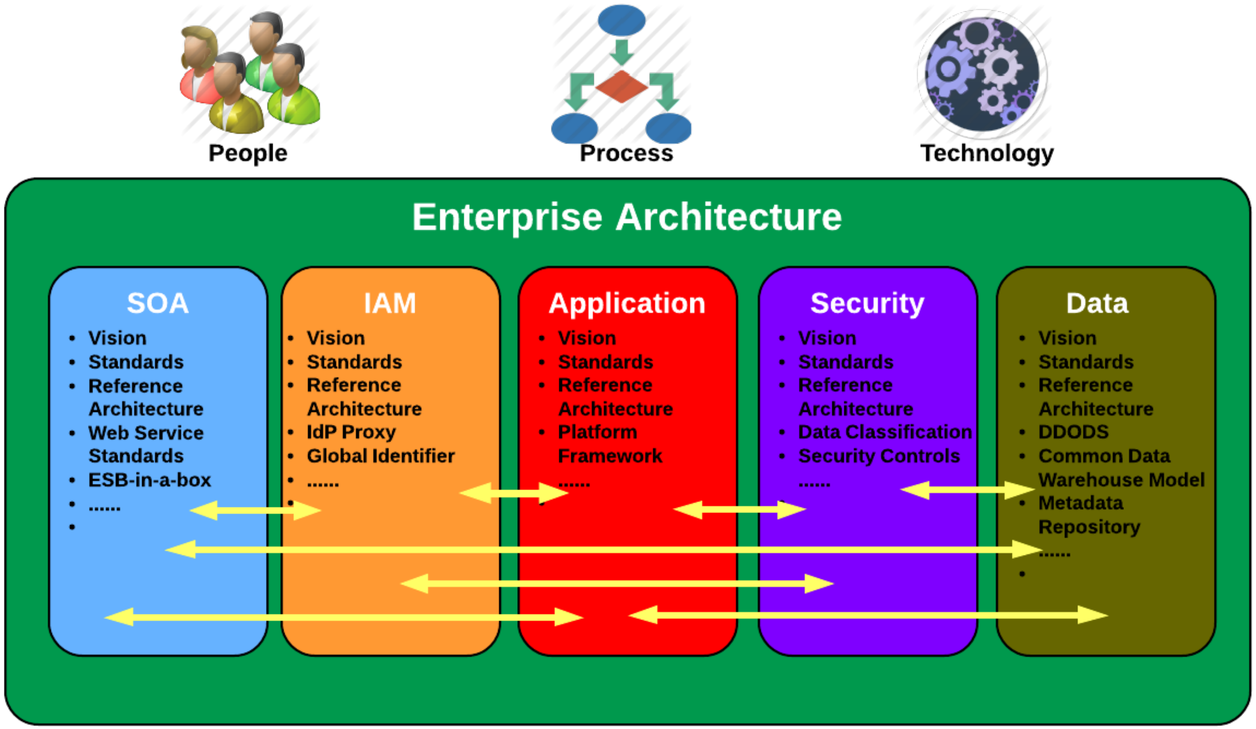
- IAM Basics
  - IAM as an element of EA
  - Brief overview of IAM
  - Federated Authentication overview
- IAM and UCOP
  - Support Federated Authentication!
  - Other Considerations for Developers and Integrators
  - UC and UCOP IAM Resources
- IAM systemwide directions
  - MFA
  - IdP Proxy
  - Global IDs
  - Data Release

IAM Basics

What is Identity and Access Management?

How Does IAM Apply to ITS?

- IAM is an area of Enterprise Architecture (EA) focus
  - EA describes significant structural components such as information, process and technology assets and how they are used to support optimized business execution.
  - EA supports shared services, interoperability and IT<->business alignment



People

Process

Technology

Enterprise Architecture

SOA
- Vision
- Standards
- Reference Architecture
- Web Service Standards
- ESB-in-a-box
- ......

IAM
- Vision
- Standards
- Reference Architecture
- IdP Proxy
- Global Identifier
- ......

Application
- Vision
- Standards
- Reference Architecture
- Platform Framework

......

Security
- Vision
- Standards
- Reference Architecture
- Data Classification
- Security Controls

......

Data
- Vision
- Standards
- Reference Architecture
- DDODS
- Common Data Warehouse Model
- Metadata Repository

......

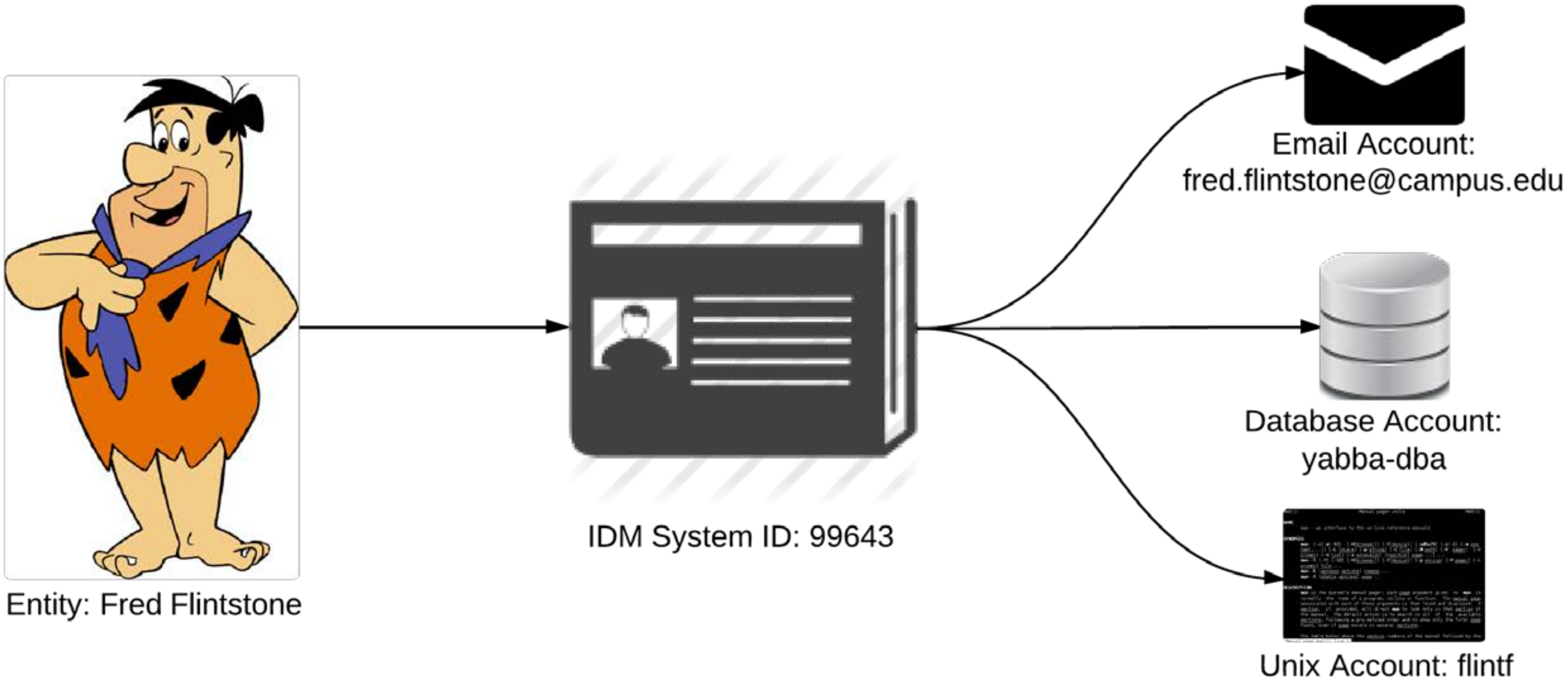
What is IAM?

- **I**dentity and **A**ccess **M**anagement
  - aka IDM, IdM or Identity Management

- Purpose of IAM
  - Ensure correct people have access to the appropriate IT resources

- Approach
  - Establish and maintain one “identity” per person
  - Central management user accounts
    - With support for Delegated and Self-Service functions
  - Provision and reconcile accounts

From Identity to Accounts



Entity: Fred Flintstone

IDM System ID: 99643

Email Account:
fred.flintstone@campus.edu

Database Account:
yabba-dba

Unix Account: flintf

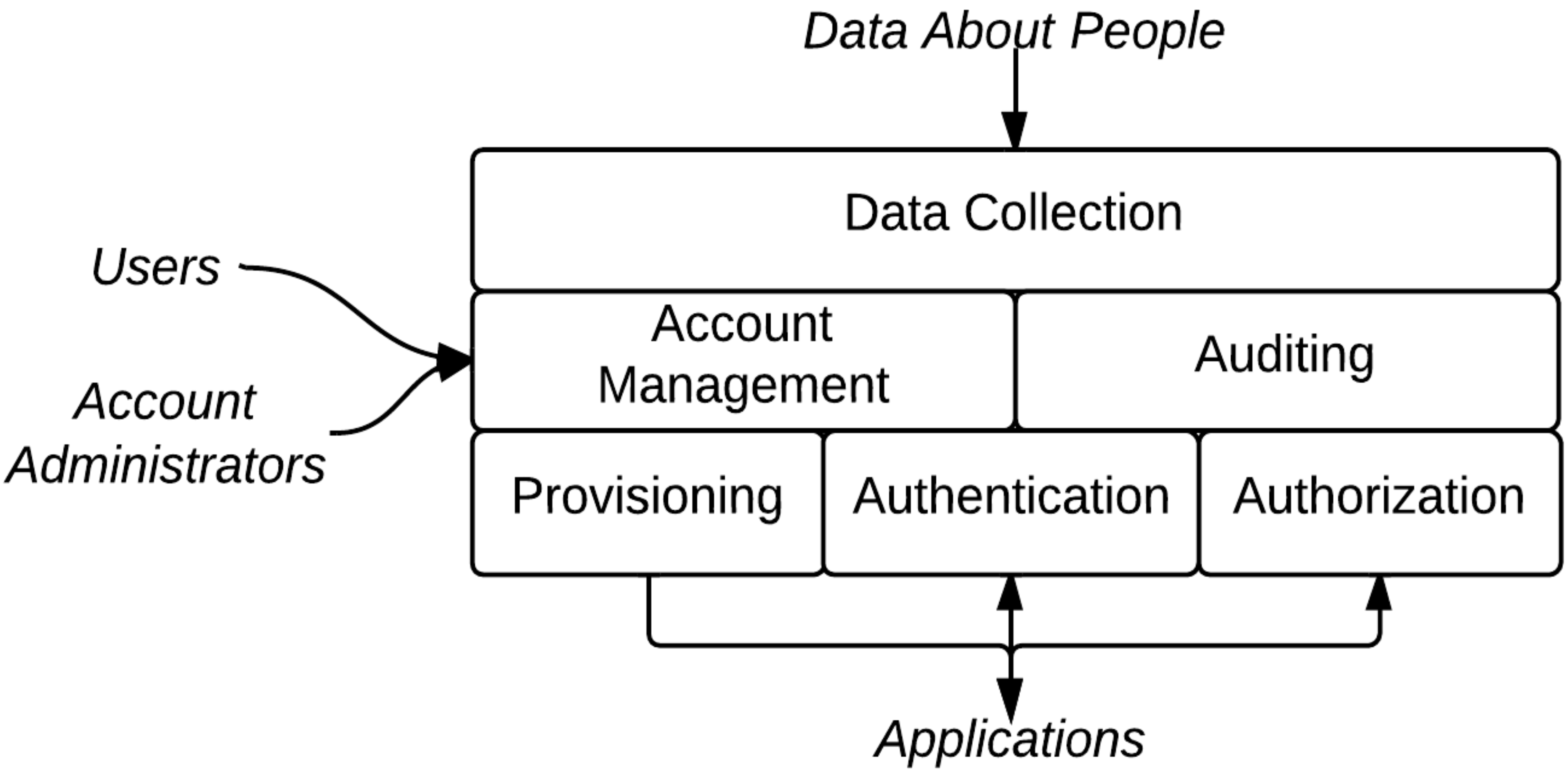
What is IAM?

- Mixture of Technology and Process

- Business Processes
  - Common business definitions
  - Service eligibility
  - Onboarding processes

- Common Technologies
  - Database, LDAP, AD, Kerberos, Grouper
  - CAS, WebAuth, Shibboleth/SAML

Elements of IAM



Elements of IAM

- Data Collection
  - Onboarding, ideally via Systems of Record (SoR)
  - "The Merge"
- Account Management
  - Administrator Account Controls
  - Self-Service Functions (Change/Reset Pwd, Data Updates)
- Auditing
  - Central logs tracking account activity/access

Elements of IAM

- Provisioning
  - Managing and reconciling accounts in external systems
- Authentication
  - Verifying who you are (aka “login”)
- Authorization
  - Privilege/permission management

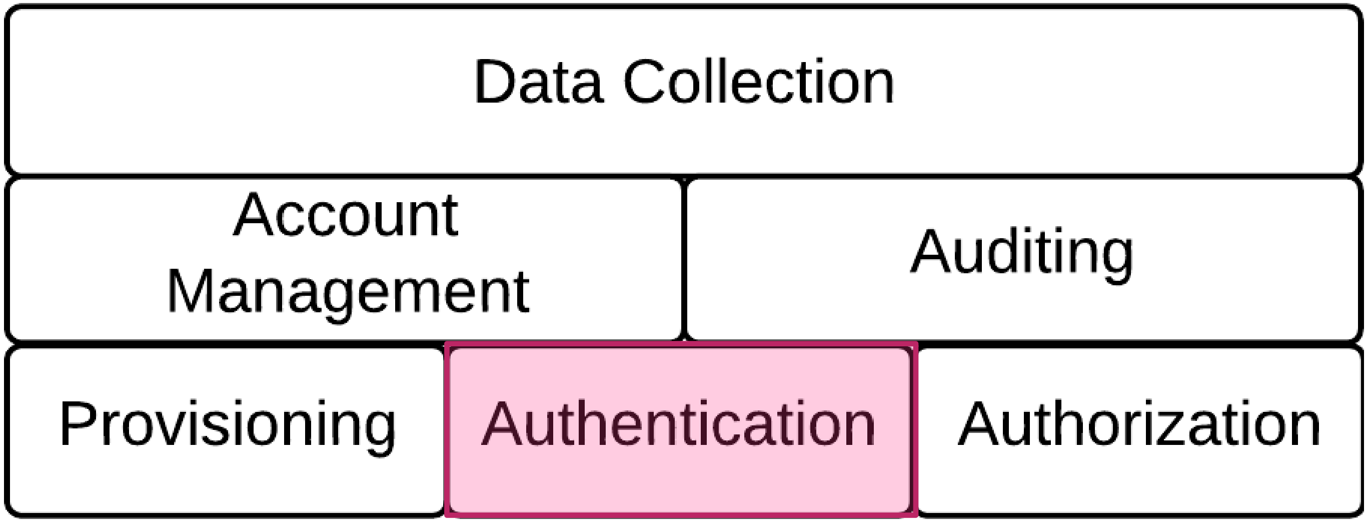
See UCPath IAM Webinar #1 (first half) for more IAM detail:

https://sp2010.ucop.edu/sites/its/ppsrepl/default.aspx

> Technical Webinars

> IAM Webinars

> 1 Identity Access Management and UCPath



Data Collection

Account Management

Auditing

Provisioning

Authentication

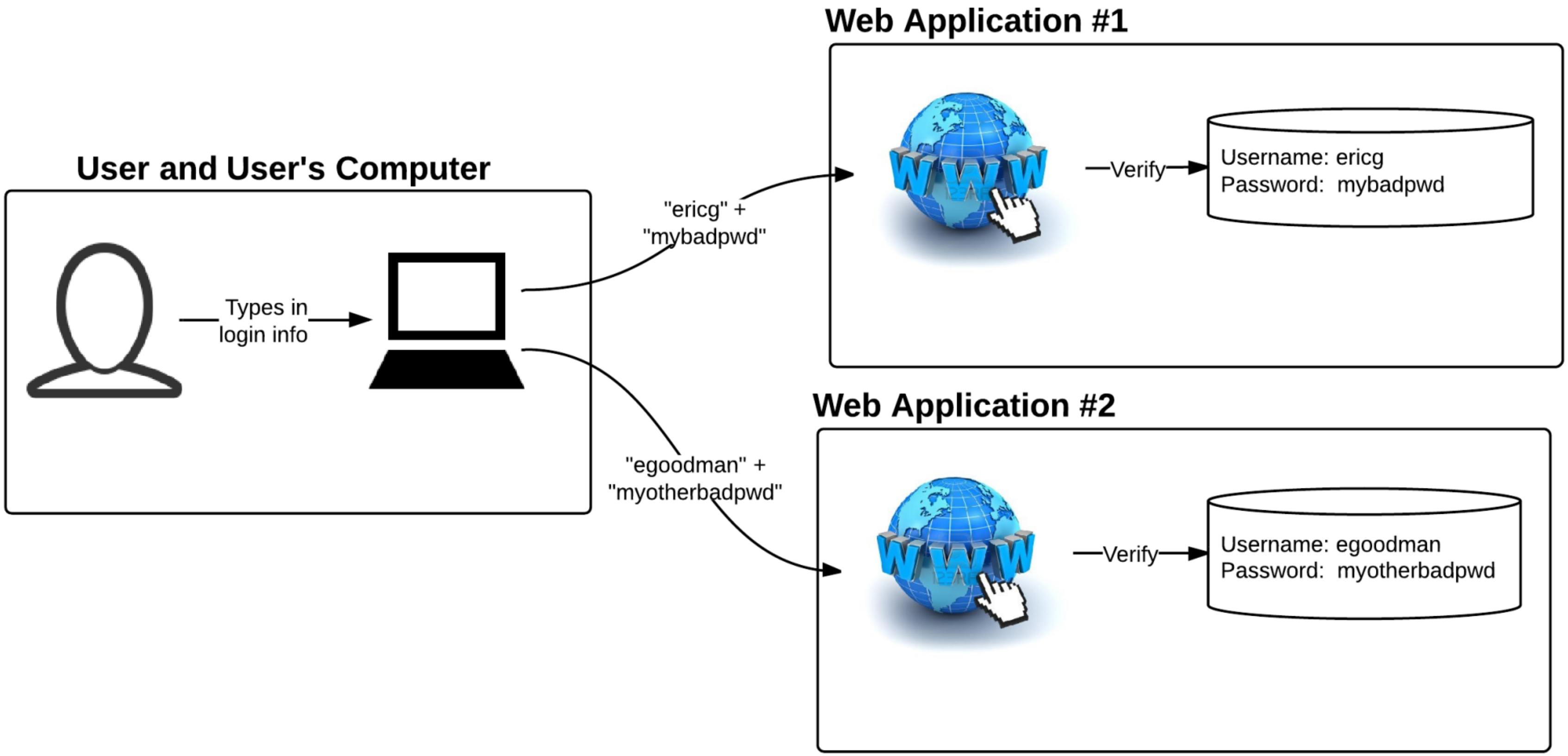
Authorization

FEDERATED AUTHENTICATION

Authentication Approaches

- Local Authentication
- Pass-thru Authentication
- Federated Authentication

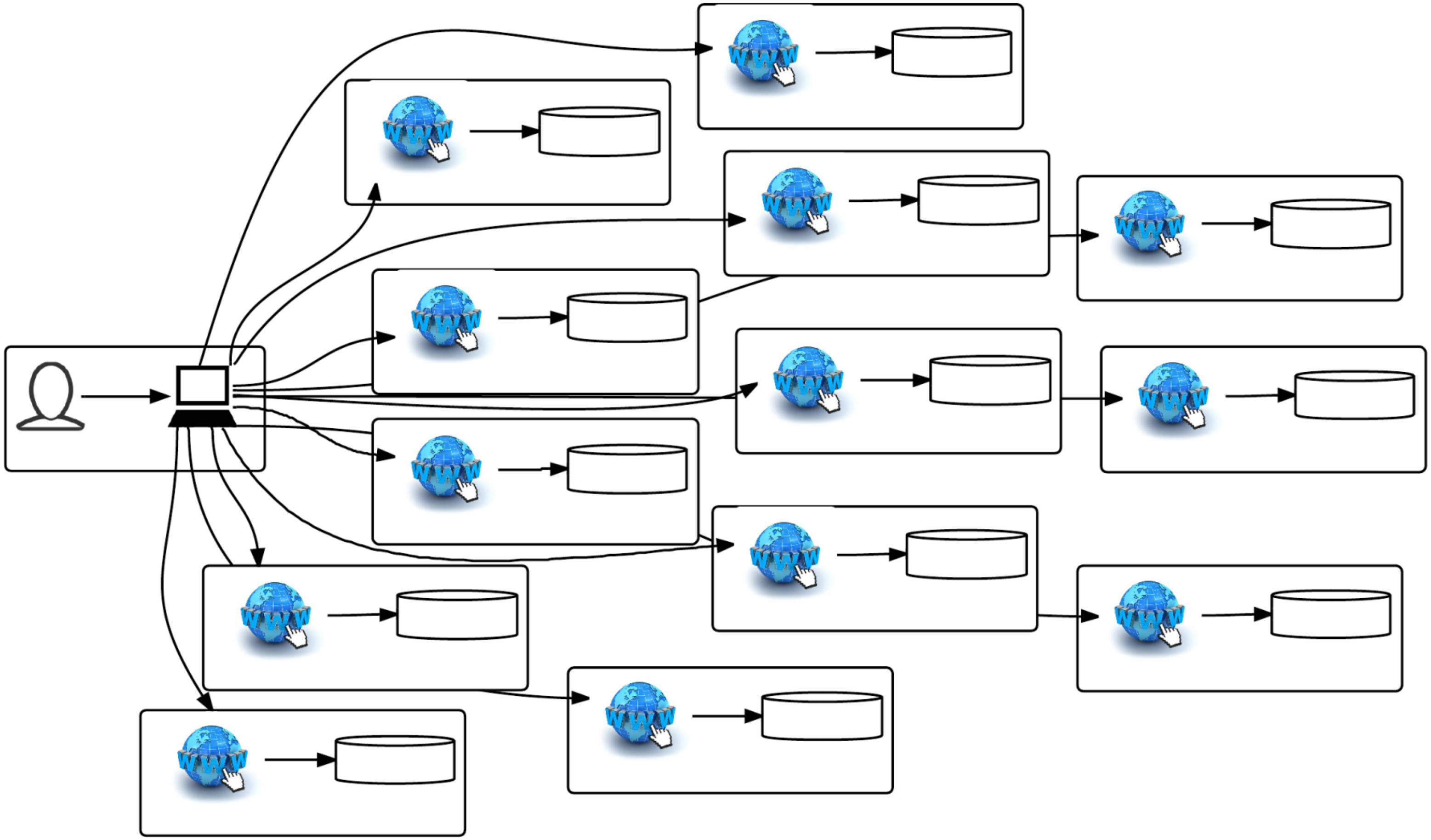
Local Authentication



Local Authentication - Scaling

- Pros
  - Flexibility
    - Different usernames and passwords for each site
  - No need to integrate with anything else
- Cons
  - Usability
    - Different usernames and passwords for each site
    - Doesn’t integrate with anything else
  - Security
    - Risk that users will reuse passwords (can’t be audited)
    - Passwords are used everywhere

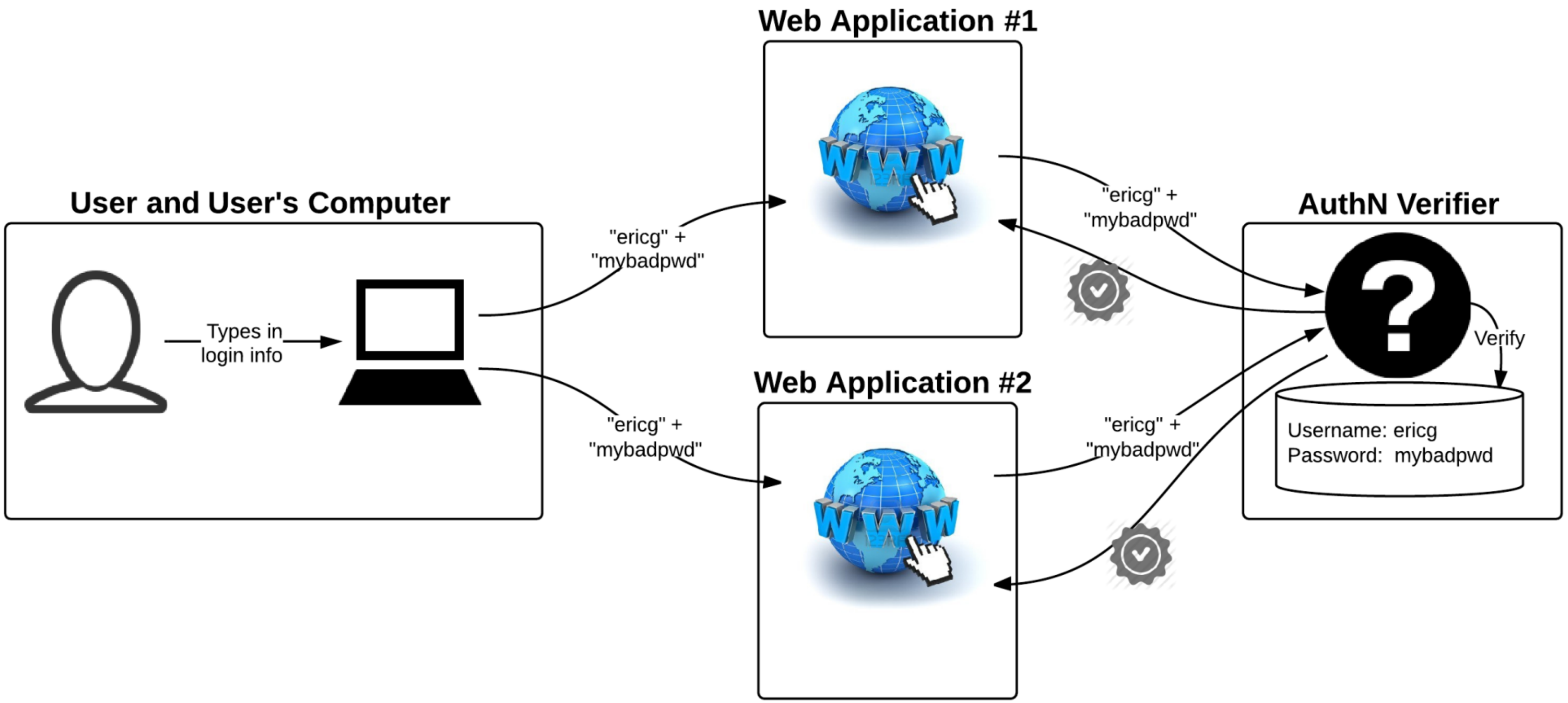
Local Authentication - Scaling



Pass-thru Authentication

“Borrowing your credentials”

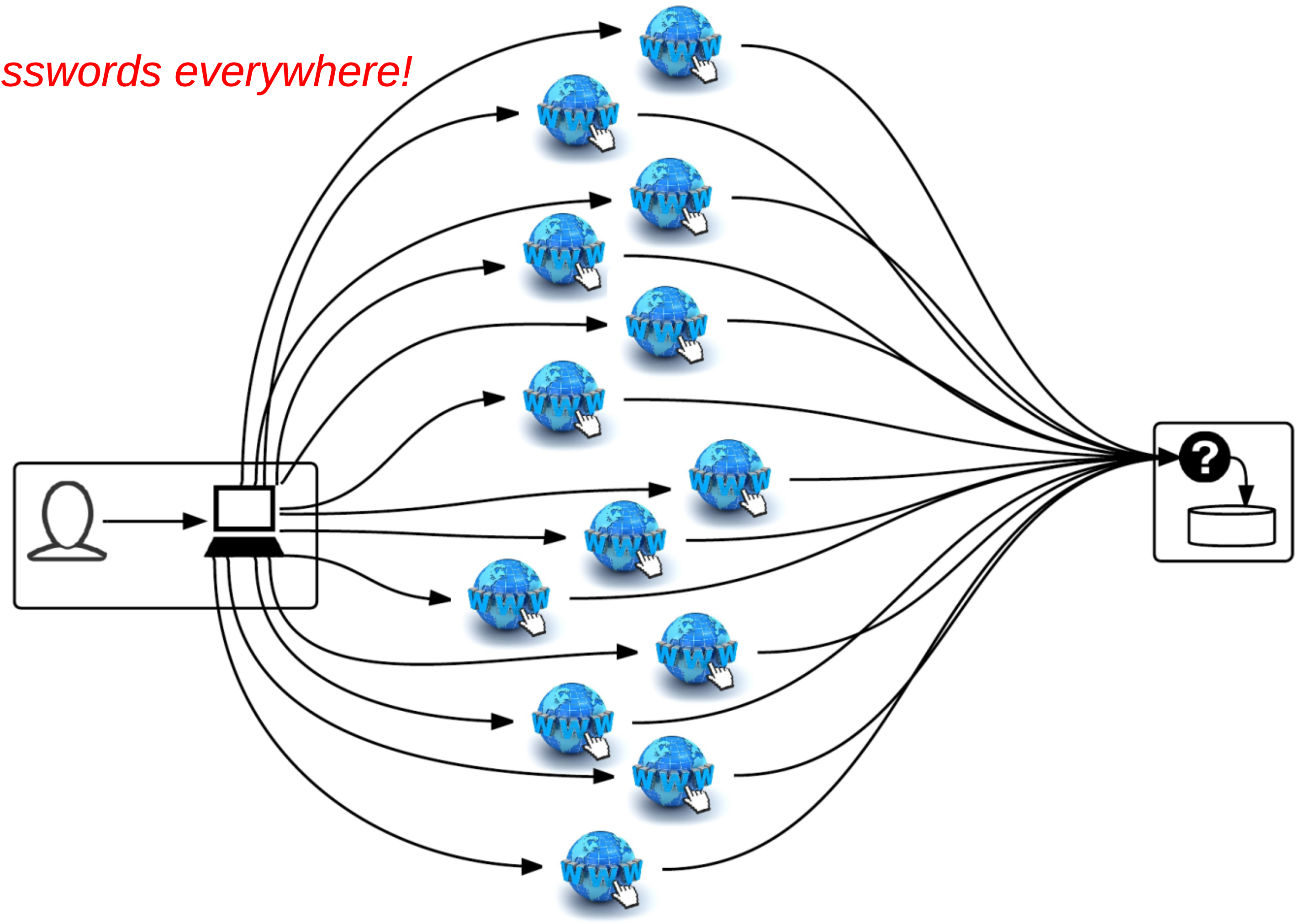
Pass-thru Authentication



Pass-thru Authentication - Scaling

- Pros
  - Consistency
    - Same username password at each site
    - Single database for account/password changes
- Cons
  - Security
    - May have to grant external applications access to internal systems
    - Many sites handle user passwords
    - Trains users to enter passwords on any web site
      - User has no way to validate website
    - Authentication service can’t distinguish you from the application
      - Application is “pretending to be you”
      - Audit, access issues

Pass-thru Authentication - Scaling



Passwords everywhere!

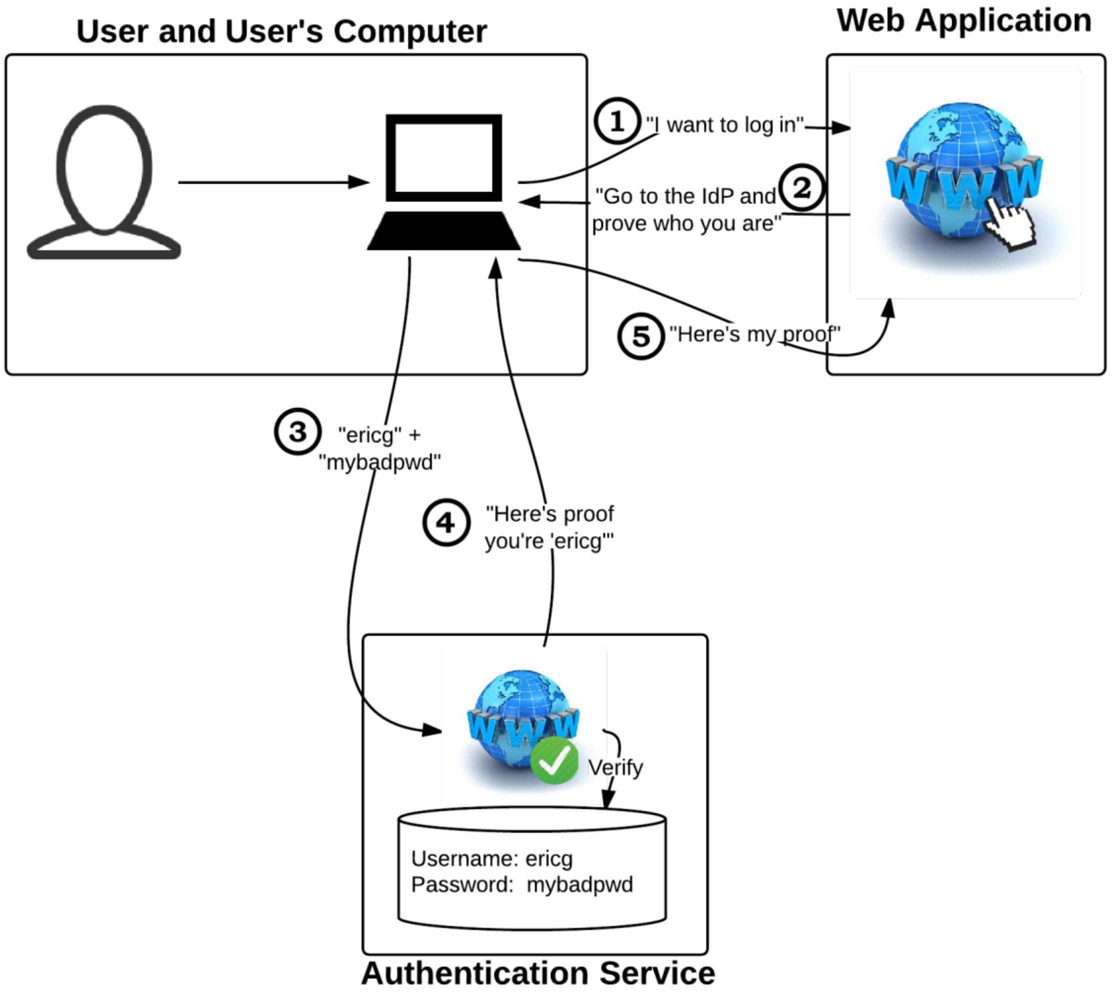
Federated Authentication

Authentication as a service

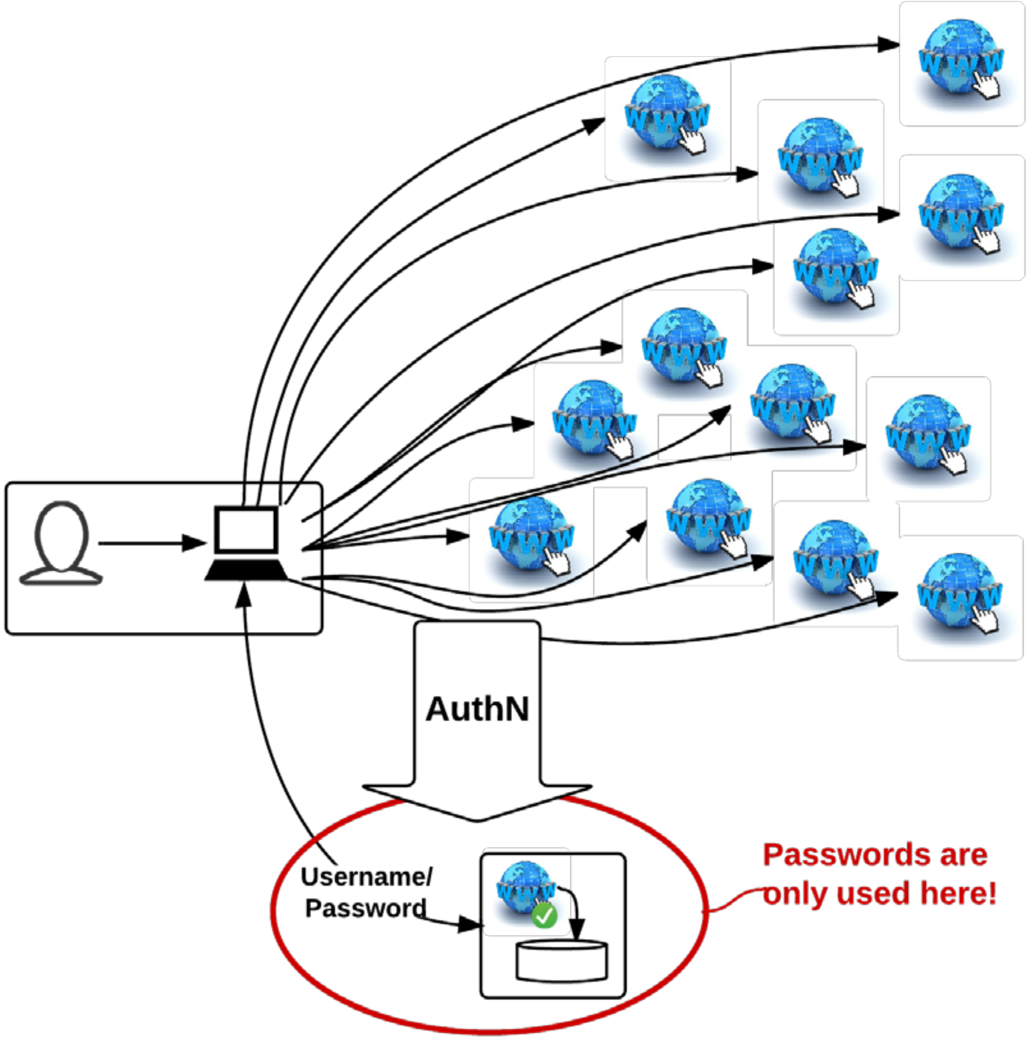
Federated AuthN

- What is Federated Authentication?
  - Isolates authentication into a separate service
  - Use your “home” account to access “remote” systems
- Federation Basics
  - Security Assertion Markup Language (SAML)
  - Shibboleth
  - Other protocols and programs exist
- Examples
  - TRS, Connexxus, LMS

Federated Authentication



Federated Authentication - Scaling



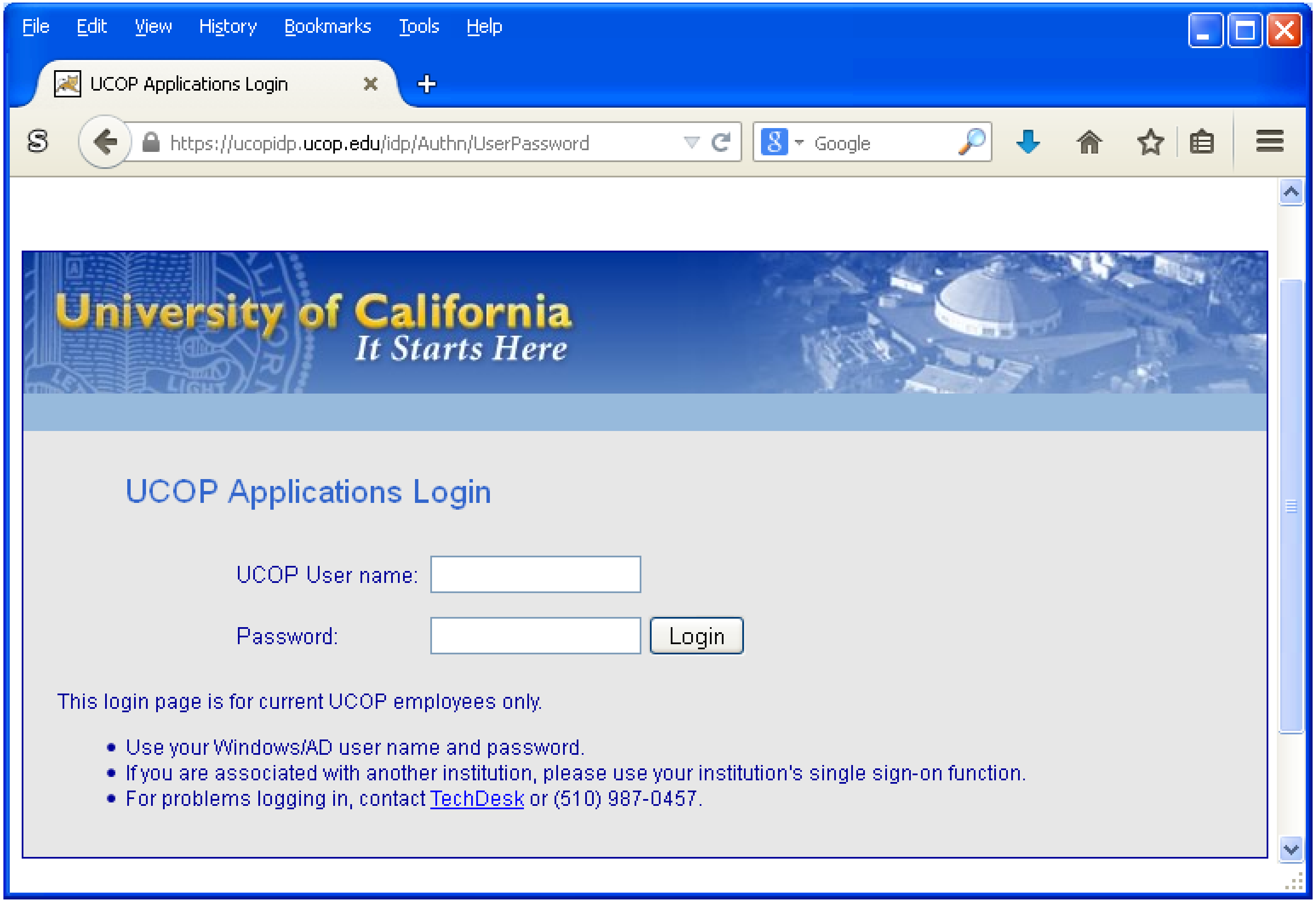
Passwords are only used here!

Federated Authentication – Scaling

- Pros
  - Security
    - Single application handles all passwords
    - Users always enter passwords on same website
  - Flexibility
    - Changes to authentication process can be handled centrally
      - Multi-factor, expired accounts
    - Provides better privacy hooks
  - Federation
    - Allows integration with multiple account stores/IdPs
      - Not limited to users from one campus

- Cons
  - Largely Web-Only
  - Learning curve is somewhat steep
  - Vendor implementations are frequently flawed

Common Login Page



UCOP Applications Login

UCOP User name:

Password:

Login

This login page is for current UCOP employees only.

- Use your Windows/AD user name and password.
- If you are associated with another institution, please use your institution's single sign-on function.
- For problems logging in, contact TechDesk or (510) 987-0457.

Federated Authentication

For more detail on Federated Authentication, see UCPath IAM Webinar #3

https://sp2010.ucop.edu/sites/its/ppsrepl/default.aspx

> Technical Webinars

> IAM Webinars

> 3 Logging Into UCPath and Federated Authentication

IAM and UCOP

What does IAM mean to me?

For New Applications

- Use Federated Authentication
  - More secure than other mechanisms
  - Especially important when working with vendors
    - Insist on SAML integration support

- Avoid Pass Thru Authentication
  - In some circumstances (esp. non-web applications) Pass-Thru may be acceptable.
  - Less secure than SAML integration

- Do not design around local accounts
  - Users are nearly guaranteed to reuse passwords
  - Adds account management burden locally

Preparing for IAM Integration

- Separate code that performs Authentication
  - Write code expecting external (SAML) Authentication

- Account != Permission
  - Rely on Roles or Attributes for access controls (RBAC/ABAC)
  - Roles and Attributes can be sourced externally

- Use defined UCTrust attributes; don’t create your own
  - https://spaces.ais.ucla.edu/display/uctrustwg/UCTrust+OIDs

IAM Resources and Organization

- UCOP IAM Team
  - Tim Hanson, Manager
  - Mark Boyce
  - Krishna Mohan
- Systemwide IAM Support
  - Eric Goodman, IAM Architect
- UCTrust
  - UC-specific “trust web” supporting Federated Authentication
- InCommon
  - Higher Ed “trust web” supporting Federated Authentication

Systemwide Directions

Projects underway or under consideration

System-wide Directions

- IdP Proxy
  - Supports vendors with limited SAML support
  - Allows for central data enhancement during authentication
- Multi-Factor Authentication
  - Various projects at different campuses
  - Desire to see more prevalent system-wide
- Global ID
  - Goal is to provide systemwide IDs across UC populations
  - Let me know if you have use cases!
- Data Release Standardization
  - Simplify process of approving and configuring data release

Question & Answer

Additional questions or consultations?

Contact *Eric Goodman, eric.goodman@ucop.edu*