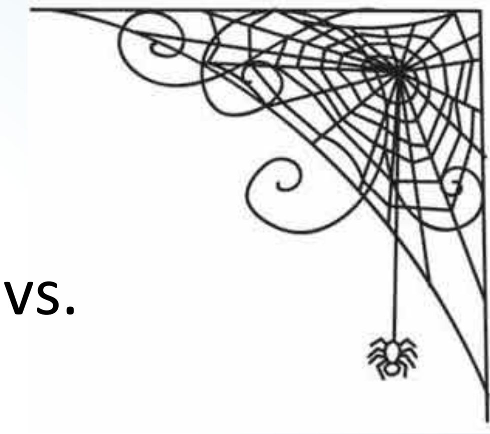
UH Applications Developers Meeting

10/31/2014

Michael Hodges, ITS, TI-IAM

Sandra Furuto, UH Data Governance

Darryl Higa, ITS, Info Sec



Agenda

- Discussion: Split Our Email List: Discussions vs. Announcements?
- Presentation: Data Governance Topics for Applications Developers
- Presentation: Test Your Web App for Obvious Security Vulnerabilities Before Going Live
- Discussion: Standardizing Attribute Release Policies for CAS and Special DNs
- Presentation: Multi-Factor Authentication Pilot Project
- Notables, Quick Tips and Reminders
- Snacks: And an opportunity to meet colleagues

Split Our App Developers Email List: Discussions vs. Announcements?

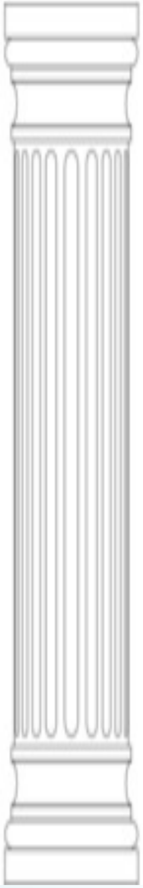
Michael Hodges

Identity and Access Management

uh-app-developers-l@lists.hawaii.edu

- Currently we have one emailing list
  - IAM posts announcements regarding IAM services
  - Members posted questions hoping for support
  - Members share success stories
- Is the one emailing list
  - To noisy?
  - Just right?
  - Still to quiet?

The Office of the Executive Vice President
for Academic Affairs



Data Governance Topics for Applications Developers

Sandra Furuto

Data Governance and Operations Director

Mandatory Training and GCN

- EP 2.215 broadly states that training and education on handling sensitive information must be completed before users are allowed access
- Proposing to update policy with specific requirements that precludes access to sensitive information, i.e., users must complete:
  - Mandatory Information Security Awareness Training
  - General Confidentiality Notice acknowledgment in ACER

Mandatory Training and GCN

- Affects users with access to unit record level data in any Institutional Data System. Examples:
  - Banner/ODS
  - Peoplesoft/HR Data Mart
  - KFS/eThority
  - STAR
  - Identity Management System
  - Etc.
- Reporting mechanism
  - Data stewards will receive a listing of individuals who have not completed either requirement

Mandatory Training and GCN

- Timeline (Tentative)
  - Approve EP 2.215 revision: early spring 2015
  - Complete reporting module: early spring 2015
  - Roll out training/GCN to current users: begin late spring 2015
  - New employee orientation requirement: ?
- Re-certification proposals
  - GCN: annually
  - Information Security Awareness Training: every 2 or 3 years

Questions?

Sandra Furuto

Data Governance and Operations Director

Test Your Web App for Obvious Security Vulnerabilities Before Going Live

Darryl Higa

Information Technology Security Specialist

Test Your Web App for Obvious Security Vulnerabilities Before Going Live

Due to the sensitivity of this material,
the slides for this presentation
are not available online.

Questions?

Darryl Higa

Information Technology Security Specialist

Standardizing Attribute Release Policies for CAS and Special DNs

Michael Hodges

Identity and Access Management

Standardizing Attribute Release Policies

- CAS attributes continue to include
  - UH Username
  - UH Number
  - First Name
  - Last Name
  - Full Name
  - Display Name
  - Affiliation (Role)
  - Campus (Organization)
  - Scope Affiliations (role@org)

Standardizing Attribute Release Policies

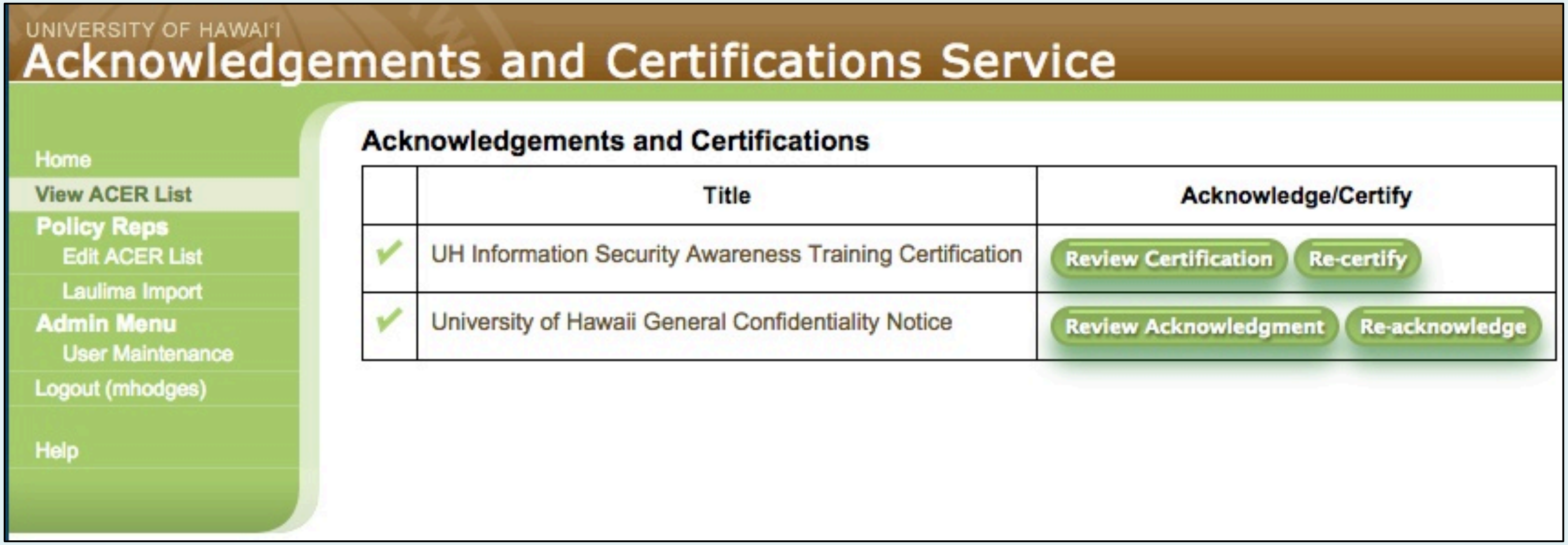
- CAS provides yet more information
  - Office FAX number
  - Personal home page URI
  - Email address(es)
  - Department Name
  - Office location
  - Office phone number
  - Job title
  - UH Acknowledgement

Standardizing Attribute Release Policies

- UH Acknowledgements and Certifications
  - Data element: uhAcknowledgement
  - Acknowledgement data includes
    - GCN, the General Confidentiality Notice
    - ISAT, Info Security Awareness Training certification
  - The Data Governance folk are discussing making the GCN and possibly the ISAT mandatory for authorizing access to sensitive information.
  - This may, ultimately, impact some of **your** applications.

Standardizing Attribute Release Policies

- UH Acknowledgements and Certifications
  - – ACER, https://www.hawaii.edu/its/acer/



UNIVERSITY OF HAWAIʻI
Acknowledgements and Certifications Service

Acknowledgements and Certifications

	Title	Acknowledge/Certify
✓	UH Information Security Awareness Training Certification	Review Certification Re-certify
✓	University of Hawaii General Confidentiality Notice	Review Acknowledgment Re-acknowledge

Standardizing Attribute Release Policies

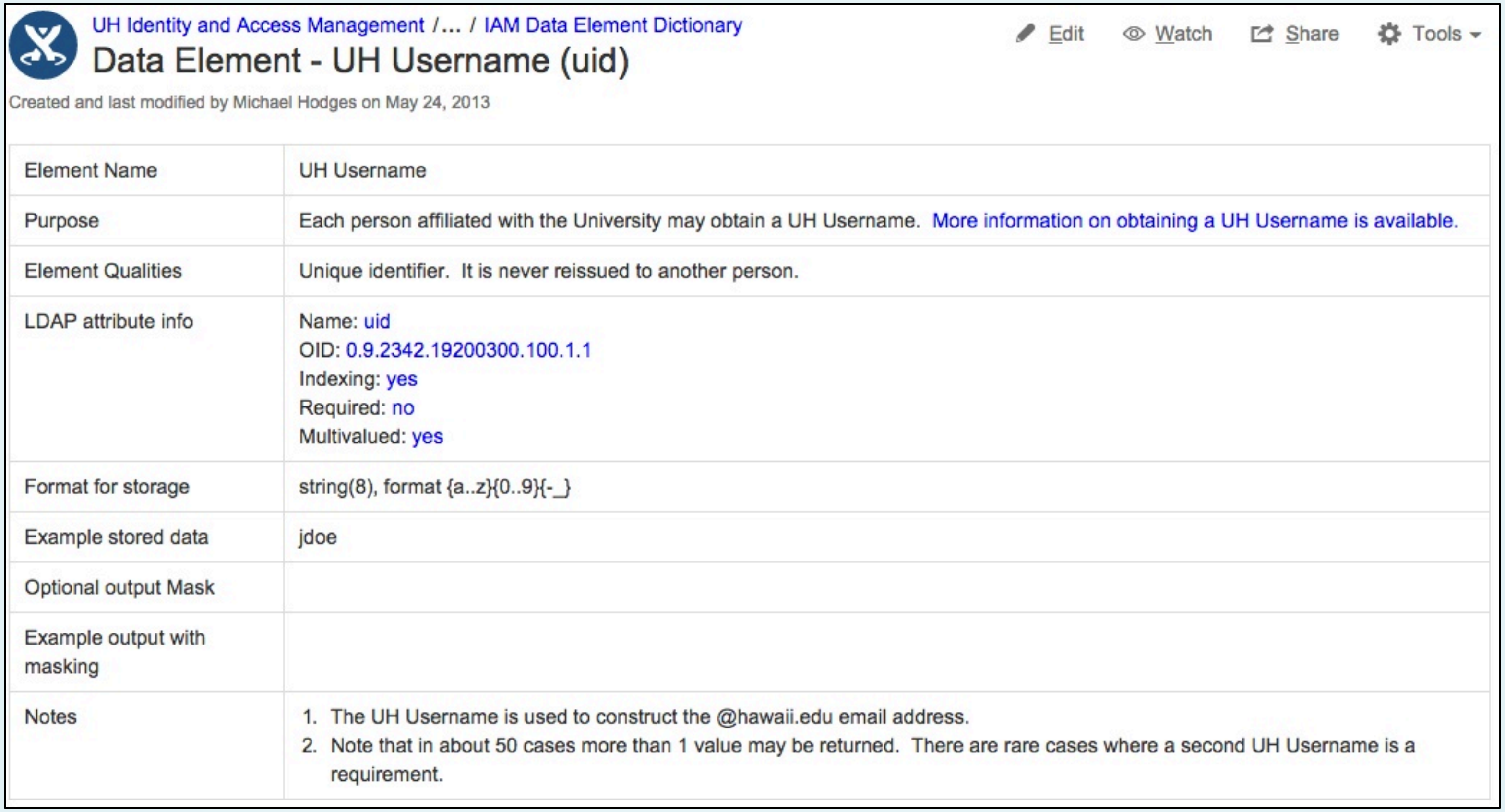
- New *DRAFT* attribute to discuss
  - Data element: uhScopedHomeOrg
  - Students and staff are each assigned a primary or home campus in the event that they are affiliated with multiple campuses.
  - Staff: campus providing the employee HR support
  - Students: primary curriculum determines campus

Standardizing Attribute Release Policies

- Known use-cases for uhScopedHomeOrg
  - AiM space management system
  - UH Manoa Space Utilization Reporting
  - UH Libraries Fee Collection Reporting
- Your use-cases?
  - *Audience participation ensues . . .*

Standardizing Attribute Release Policies

- An IAM Data Element Dictionary is available.
  - Search bwiki for "IAM Data"



UH Identity and Access Management / ... / IAM Data Element Dictionary
Edit
Watch
Share
Tools

Data Element - UH Username (uid)

Created and last modified by Michael Hodges on May 24, 2013

Element Name	UH Username
Purpose	Each person affiliated with the University may obtain a UH Username. More information on obtaining a UH Username is available.
Element Qualities	Unique identifier. It is never reissued to another person.
LDAP attribute info	Name: uid OID: 0.9.2342.19200300.100.1.1 Indexing: yes Required: no Multivalued: yes
Format for storage	string(8), format {a..z}{0..9}{-_}
Example stored data	jdoe
Optional output Mask	
Example output with masking	
Notes	1. The UH Username is used to construct the @hawaii.edu email address. 2. Note that in about 50 cases more than 1 value may be returned. There are rare cases where a second UH Username is a requirement.

IAM Data Element URLs

- IAM Data Element Dictionary:
  - https://www.hawaii.edu/bwiki/display/UHIAM/IAM+Data+Element+Dictionary
- Draft IAM Data Element uhScopedHomeOrg:
  - https://www.hawaii.edu/bwiki/pages/viewpage.action?pageId=279937086
- New IAM Data Element uhAcknowledgement:
  - https://www.hawaii.edu/bwiki/pages/viewpage.action?pageId=266174513

Questions?

Michael Hodges

Identity and Access Management

Multi-Factor Authentication Pilot Project

Michael Hodges

Identity and Access Management

Multi-Factor Authentication

Knowledge

Possession

Inherence

Multi-Factor Authentication

- **Authentication**
  - Proving that you are who you say you are.
- **Authentication factors** used for proof
  - Knowledge factor
    - Something I know (username/password)
  - Possession factor
    - Something I have (token, phone)
  - Inherence factor
    - Something I am (fingerprint, iris pattern)

Multi-Factor Authentication

- Issues as discussed with our IT auditors
  - **1-step authentication**, knowledge,
    - Password-guessing mitigation requires advanced password-complexity requirements, password expiration dates, and reuse must be prevented.
  - **2-step**, knowledge + knowledge, +
    - The 2nd step usually involves personalized questions.
    - The 2nd step requires well-designed questions, expiration dates and and reuse must be prevented.
  - **Multi-factor**, knowledge + possession, +
    - No issues, if done well

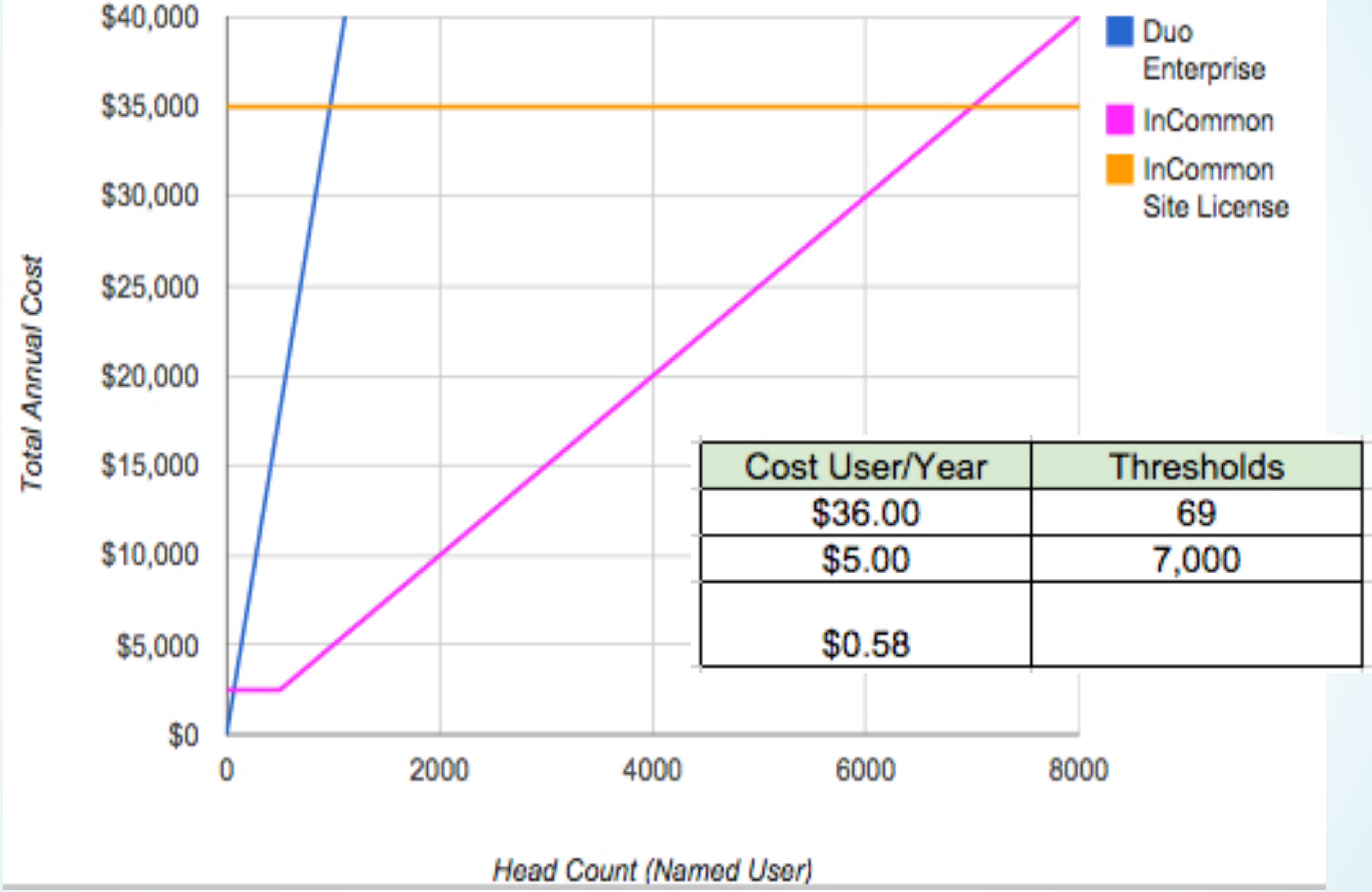
Multi-Factor Authentication

- Requirements for implementation:
  - – Easy to implement
  - – Easy to deploy
  - – Easy to use, by everyone
  - – Easy to support, self-service functions are essential
  - – Very easy to scale up
  - – Very cost effective
  - – Accessible to our app developer community

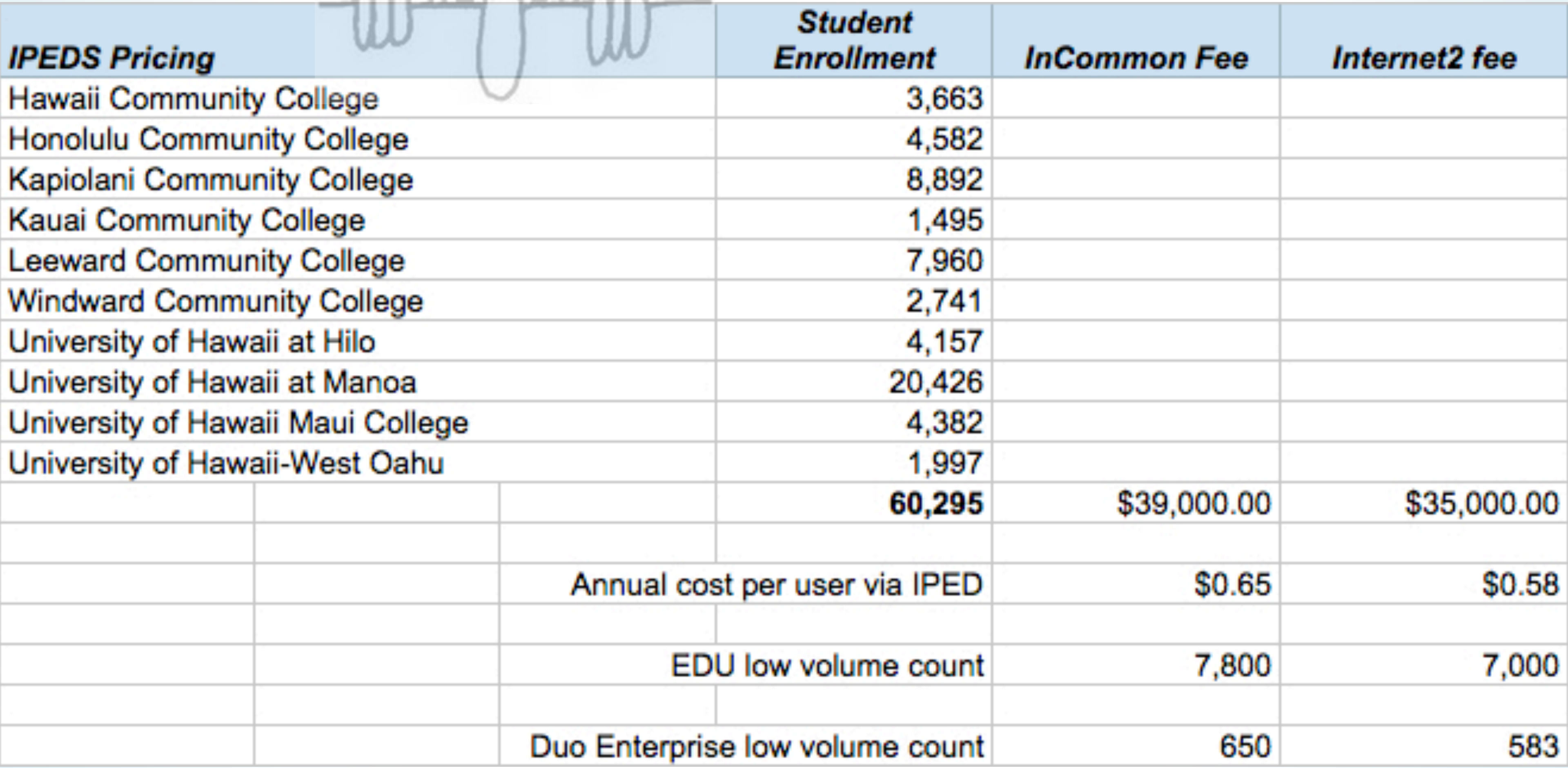
Multi-Factor Authentication

- Solution: Duo Security
  - The service is cloud-based
    - Easy to implement
    - Easy to deploy
    - Easy to scale up
  - Software, self-service functions and docs are provided
    - Easy to use, by everyone *(mostly)*
    - Easy to support
    - Accessible to our app developer community
  - Deep discounts provided to Higher Ed
    - Very cost effective.

Head Count Cost Projections by Licensing Model



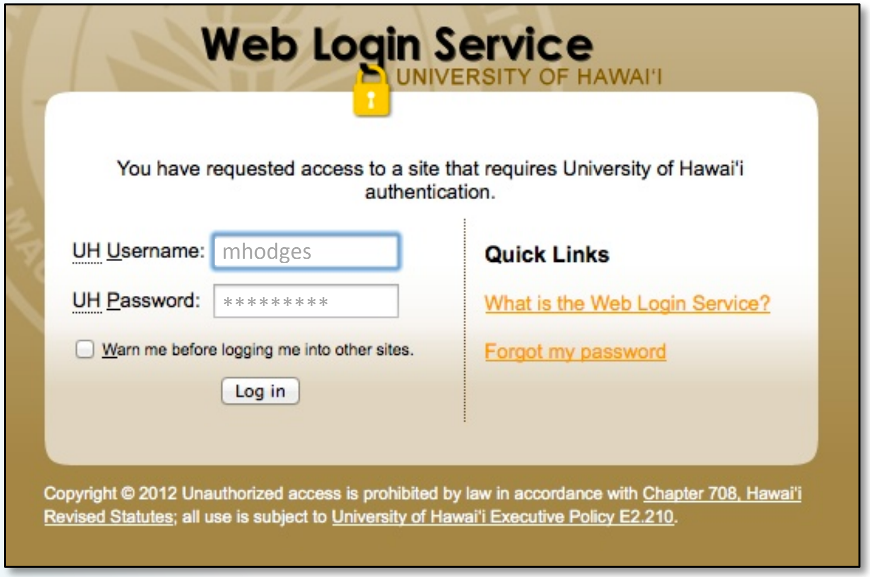
Cost User/Year	Thresholds
$36.00	69
$5.00	7,000
$0.58	



IPEDS Pricing	Student Enrollment	InCommon Fee	Internet2 fee
Hawaii Community College	3,663		
Honolulu Community College	4,582		
Kapiolani Community College	8,892		
Kauai Community College	1,495		
Leeward Community College	7,960		
Windward Community College	2,741		
University of Hawaii at Hilo	4,157		
University of Hawaii at Manoa	20,426		
University of Hawaii Maui College	4,382		
University of Hawaii-West Oahu	1,997		
	60,295	$39,000.00	$35,000.00
Annual cost per user via IPED		$0.65	$0.58
EDU low volume count		7,800	7,000
Duo Enterprise low volume count		650	583

Multi-Factor Authentication

What multi-factor authentication would look at UH



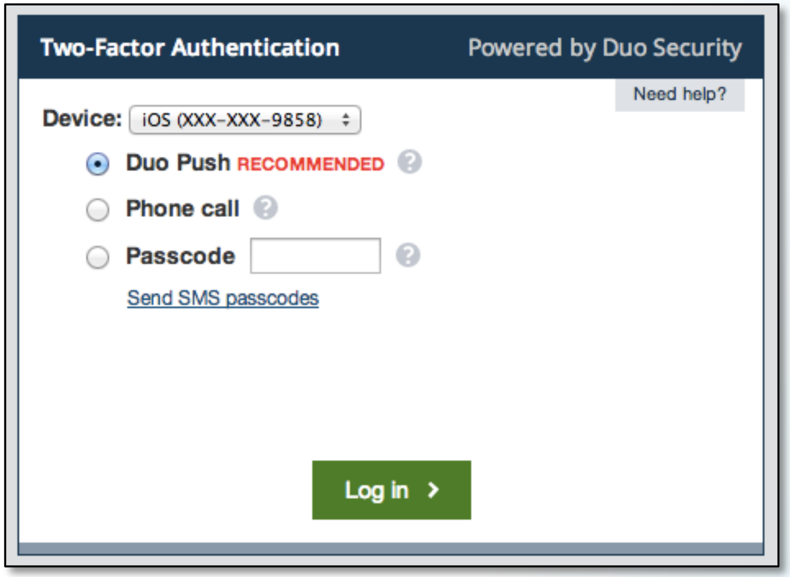
You have requested access to a site that requires University of Hawai'i authentication.

UH Username: mhodges

UH Password: *********

□ Warn me before logging me into other sites.

Copyright © 2012 Unauthorized access is prohibited by law in accordance with Chapter 708, Hawai'i Revised Statutes; all use is subject to University of Hawai'i Executive Policy E2.210.



Device: iOS (XXX-XXX-9858)

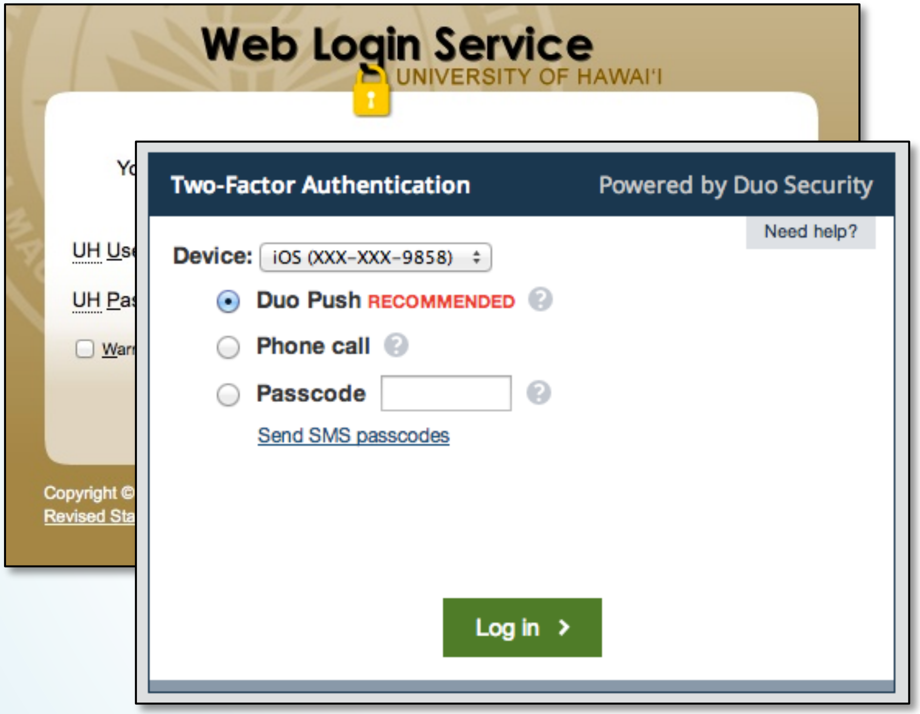
● Duo Push RECOMMENDED

○ Phone call

○ Passcode

Multi-Factor Authentication

Knowledge



Web Login Service

UNIVERSITY OF HAWAI'I

Yo

UH Use

UH Pas

□ Warn

Copyright ©

Revised Sta

Two-Factor Authentication Powered by Duo Security

Need help?

Device: iOS (XXX-XXX-9858)

● Duo Push RECOMMENDED

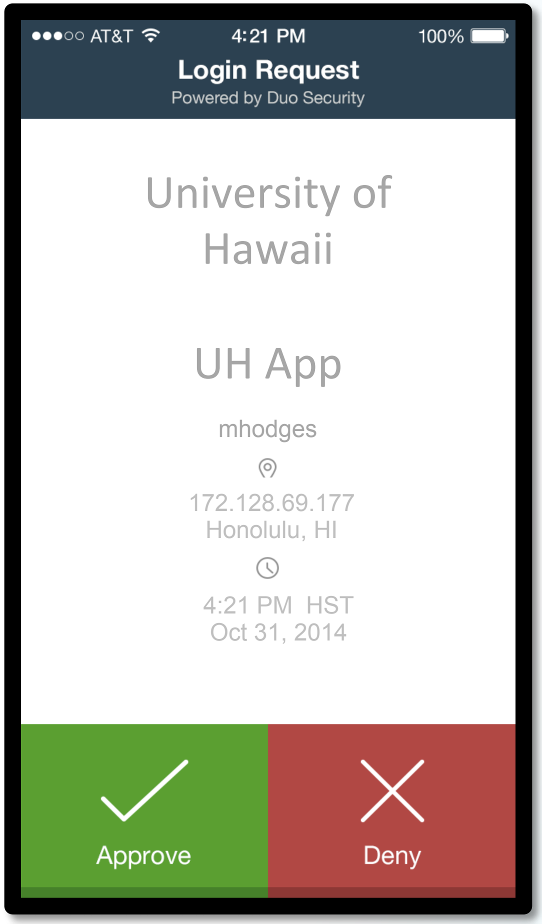
○ Phone call

○ Passcode

Send SMS passcodes

Log in ›

+



●●●○○ AT&T 4:21 PM 100%

Login Request

Powered by Duo Security

University of Hawaii

UH App

mhodges

172.128.69.177
Honolulu, HI

4:21 PM HST
Oct 31, 2014

✓ Approve

✗ Deny

Possession

Multi-Factor Authentication URLs

- How much security is enough?
  - https://wiki.cohortium.internet2.edu/confluence/pages/viewpage.action?pageId=4915231
- The quest to replace passwords:
  - https://www.lightbluetouchpaper.org/2012/05/22/the-quest-to-replace-passwords/
- Wikipedia article:
  - http://en.wikipedia.org/wiki/Multi-factor_authentication
- Duo Security Guide to 2-Factor Authentication
  - http://guide.duosecurity.com/

Questions?

Michael Hodges

Identity and Access Management

Notables & Reminders

Michael Hodges

Identity and Access Management

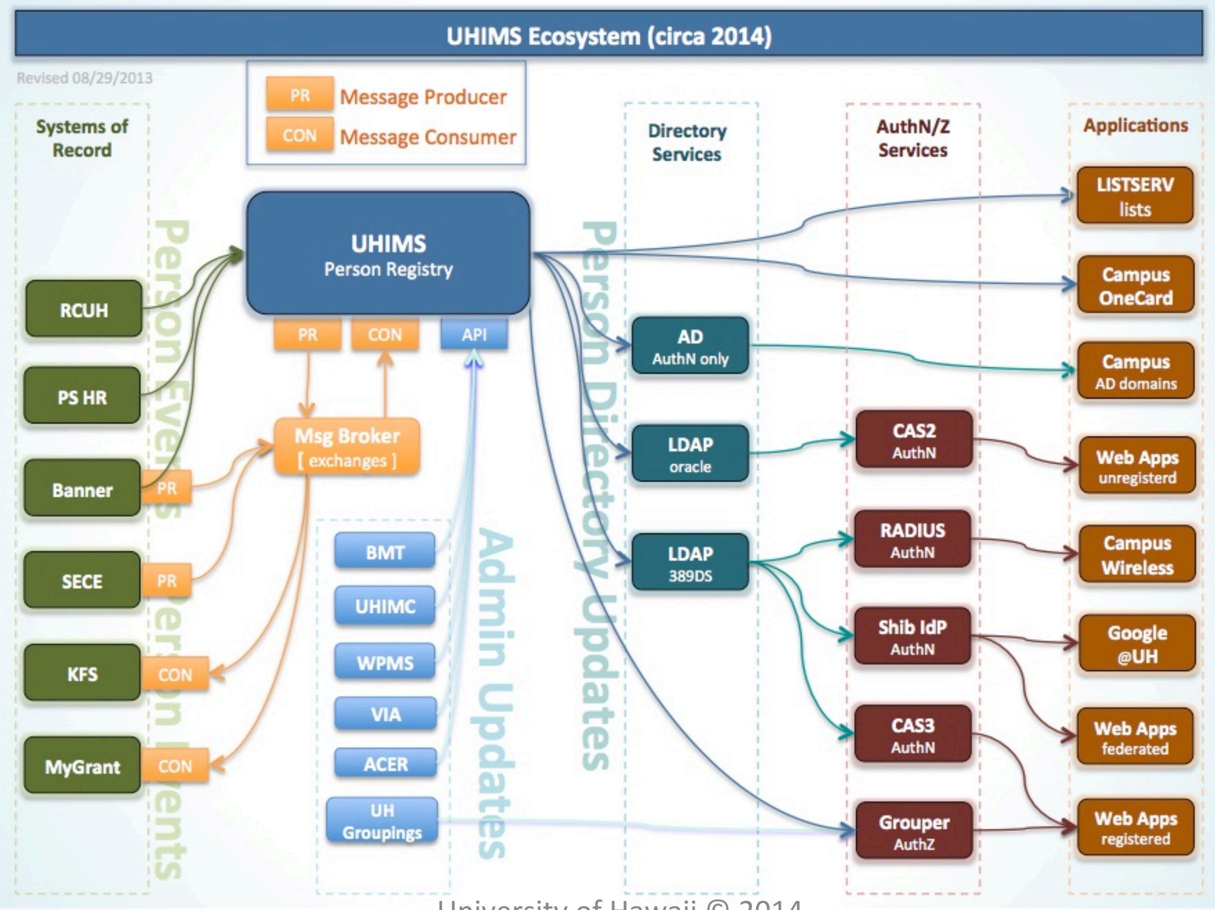
Notables

- UH Applications Developers LISTSERV List
  - Membership is over 198 people and growing.

- Applications registered to use CAS for AuthN:
  - Registered apps is over 195 URLs and growing

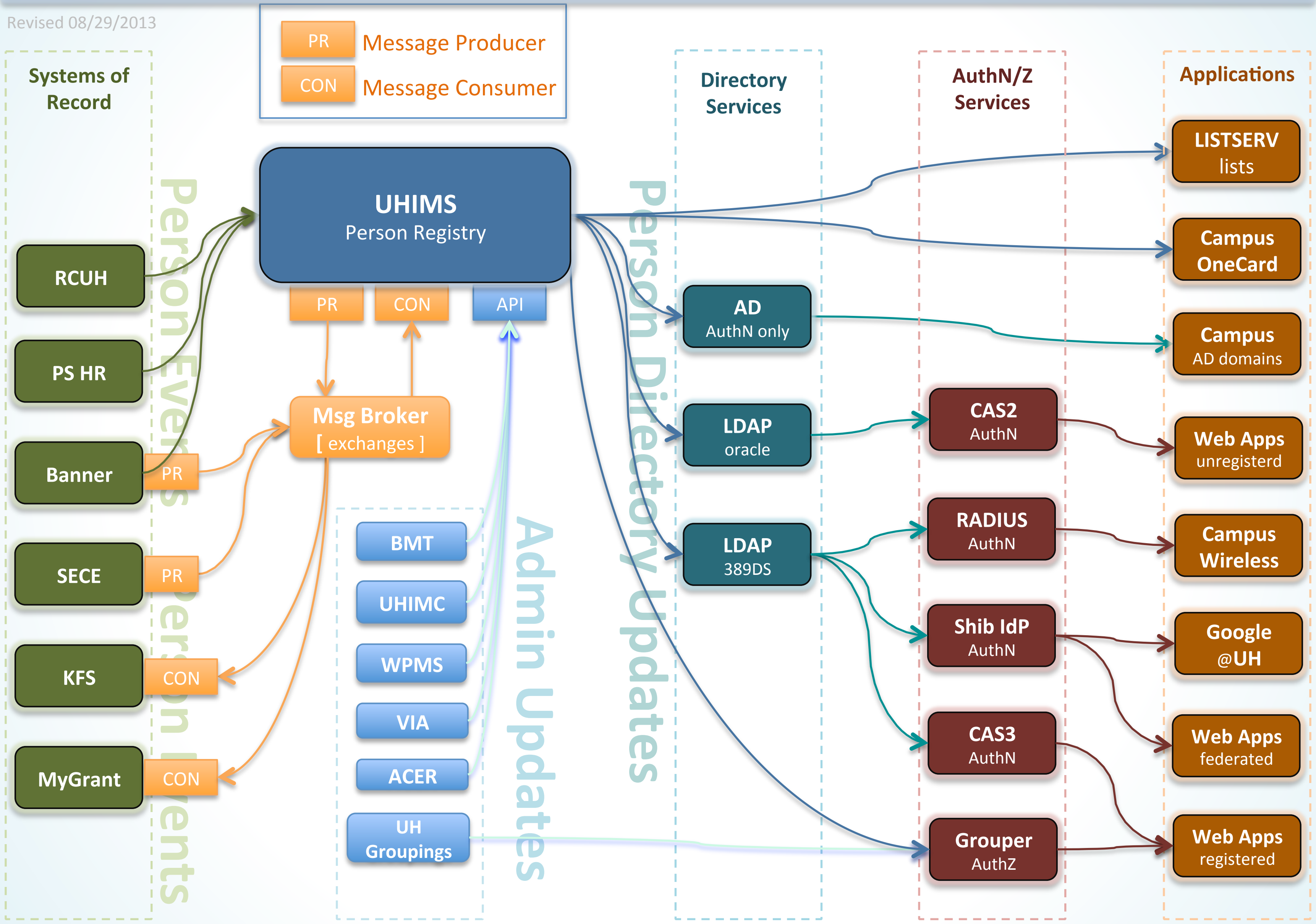
End of Service Life Reminders

- Legacy **CAS2** & **LDAP** – EOSL is **12/31/2014**



UHIMS Ecosystem (circa 2014)

Revised 08/29/2013



PR Message Producer

CON Message Consumer

Systems of Record

RCUH

PS HR

Banner PR

SECE PR

KFS CON

MyGrant CON

Person Events

UHIMS Person Registry

PR CON API

Msg Broker [exchanges]

BMT

UHIMC

WPMS

VIA

ACER

UH Groupings

Admin Updates

Person Directory Updates

Directory Services

AD AuthN only

LDAP oracle

LDAP 389DS

AuthN/Z Services

CAS2 AuthN

RADIUS AuthN

Shib IdP AuthN

CAS3 AuthN

Grouper AuthZ

Applications

LISTSERV lists

Campus OneCard

Campus AD domains

Web Apps unregisterd

Campus Wireless

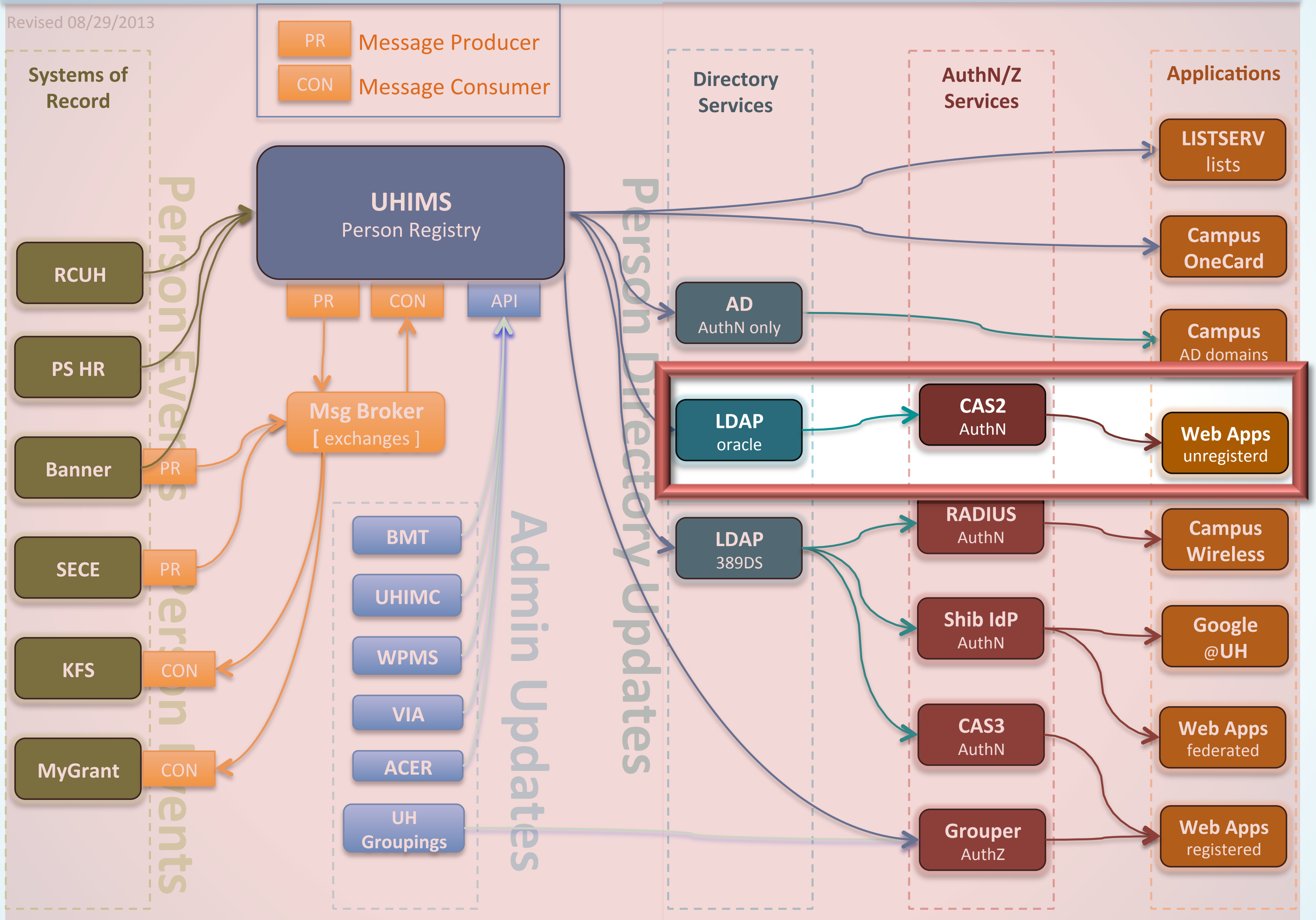
Google @UH

Web Apps federated

Web Apps registered

UHIMS Ecosystem (circa 2014)

Revised 08/29/2013



Questions?

Note that we have attempted to capture the questions & answers and will publish what we've snagged along with these slides.

https://www.hawaii.edu/bwiki/display/UHIAM/UH+Applications+Developers+forum

Wrapping Up

- Happy Halloween!!!
- Email suggestions for future topics to mhodges@hawaii.edu
- Check out the snacks in the back
- Take a moment to introduce yourself to your colleagues (meet at least 1 new person)