UH Applications Developers Meeting
2/10/2012

Michael Hodges, ITS, IAM
Stephan Fabel, UHM, COE

Agenda

- Poll: UH Developers listserv list
- Update: Quick status update
- Poll: Determine boot camp interest
- **Presentation**: Using LDAP and SASL
- Factoid: UH Number / UH Username
- Factoid: OID Assignments
- **Presentation**: LDAP changes

UH App Devs Meeting

- Poll:

  UH Developers listserv list
  - Establish an online forum for UH Developers?

UH App Devs Meeting

- Update:

  Quick status update for previously mentioned projects:

  - UHIMS Grouper
  - UHIMS Events
  - ACER
  - LDAP Pruning

UH App Devs Meeting

- Update:
  - UHIMS Grouper
    - In Production for the targeted Daily Termination Reports
      - ITS and UHM Parking Office currently, others planed
      - Grouper audit logs proving useful for IT audits
    - Automatic groups not yet ready
    - Grouper CASification planned
    - Grouper upgrade to a current release is planned
      - GUI support for custom attributes
    - Boot camps anyone?

    - Why is it important to UH Developers?
      - RBAC!!! When authentication is not enough!

UH App Devs Meeting

- Update:
  - UHIMS Events
    - UHIMS Messaging standards implemented
    - White Pages Management System incorporated
    - Will be used to publish events for consumption by the Kuali Financials
    - High Availability infrastructure will be in Production before end of month (Feb 2012)
    - Why is it important to UH Developers?
      - RBAC!!! When authentication is not enough!

UH App Devs Meeting

- Update:
  - ACER – Acknowledgements and Certifications
    - Prototype to be completed by end of Feb 2012
    - Pilots to include:
      - General Confidentiality Notice
      - UH Information Security Awareness Training
      - ACER RBAC in UHIMC
    - Why is it important to UH Developers?
      - RBAC!!! When authentication is not enough!

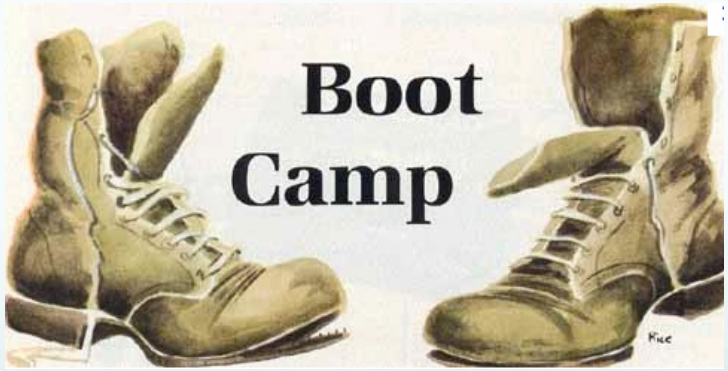
UH App Devs Meeting

- Update:
  - LDAP Pruning
    - Planned for the upcoming LDAP project
    - Gotcha for us to track: developer expectations that LDAP holds the entire list of UH Numbers and Usernames.
      - If this is useful, an alternative strategy, such as a web service would be considered.

UH App Devs Meeting

- Poll:

  Determine interest in hands-on UHIMS Events and UHIMS Grouper boot camps



UH App Devs Meeting

- Presentation:

  Using LDAP (AuthZ) and SASL (AuthN) for pass-through authentication to control lab computers access

UH App Devs Meeting

- Factoid:

  UH Number or UH Username, which is the recommended unique identifier for applications?

  (spoiler alert, the numeric one)

UH App Devs Meeting

- Factoid:

  Coordinating OID (object identifier) Requests and Assignments for the UH Developer Community by providing:

  - OID Preassingments
    - UH is assigned 1.3.6.1.4.2160 by IANA
    - Honolulu; 1.3.6.1.4.2160.63 by ITS
  - Process for registering Campus OIDs
  - Central repository of OID assignments
    - https://www.hawaii.edu/bwiki/display/UHIAM

UH App Devs Meeting

- Presentation:

  Planned LDAP infrastructure changes to enhance availability and scalability

LDAP Infrastructure and Authentication

LDAP to become:

More robust

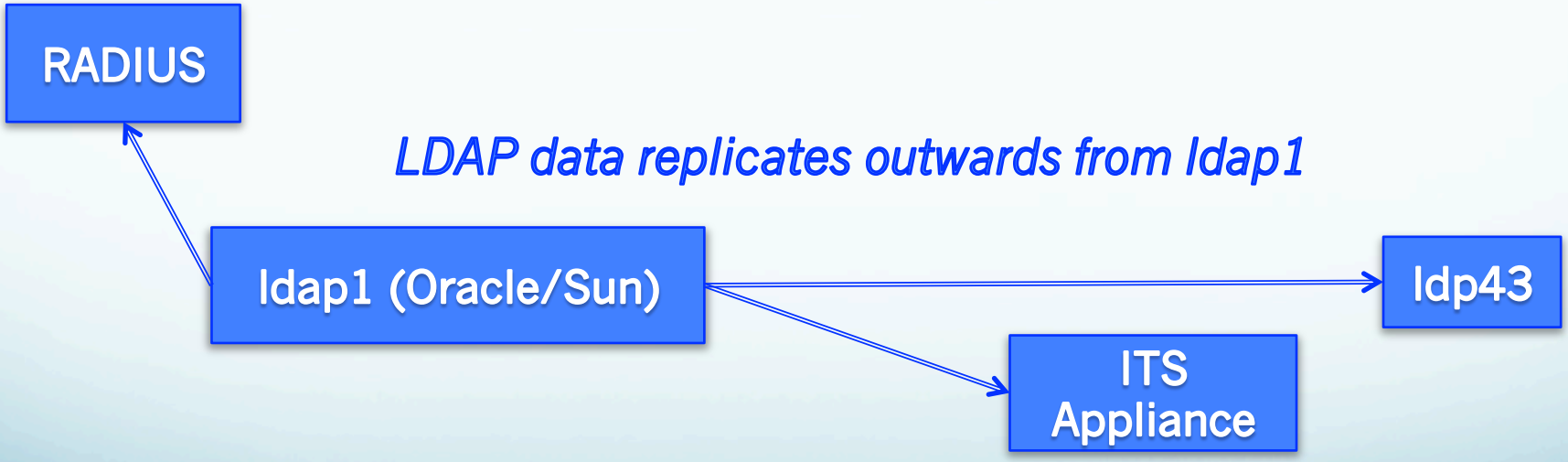
More secure

More scalable

LDAP for AuthN Today

Backend Authentication Components

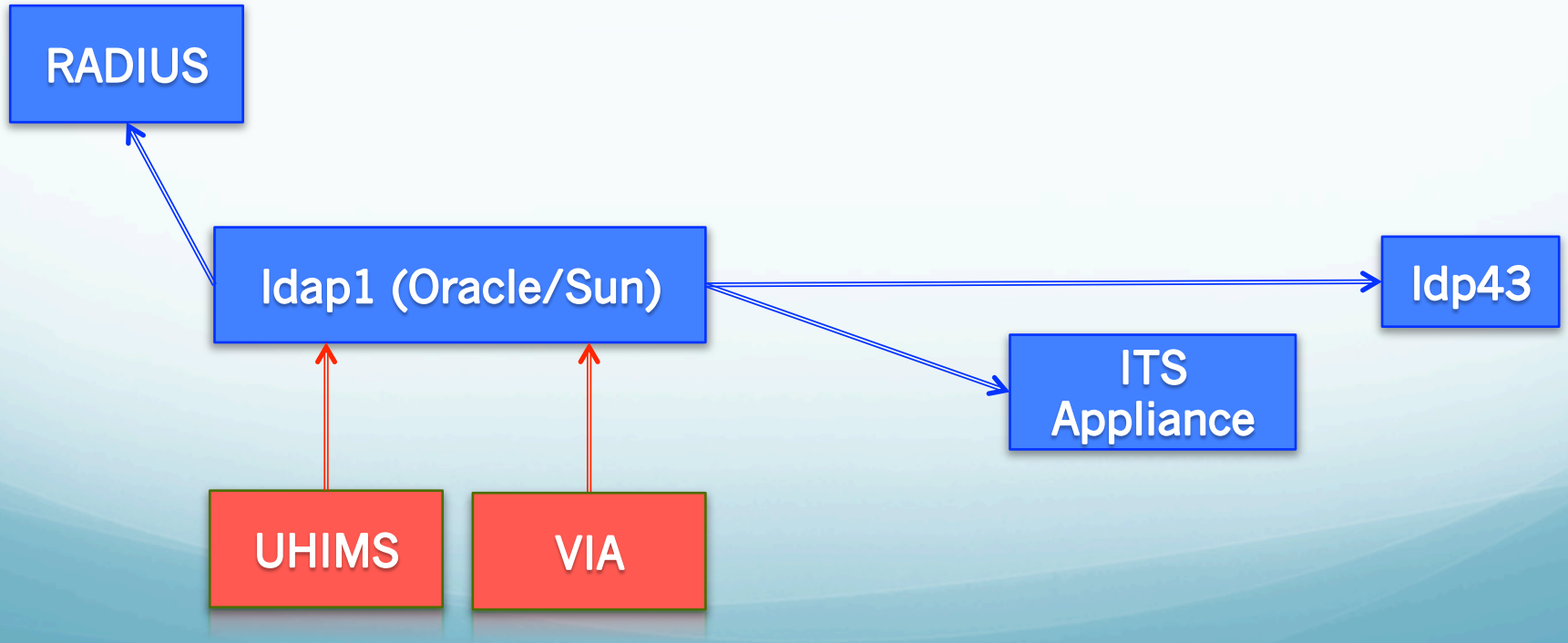
- RADIUS – redundant infrastructure for High Availability
- LDAP – very redundant infrastructure for High Availability
- ITS Appliance – replicates LDAP outside the UH data center



LDAP for AuthN Today

Identity and Access Management Components

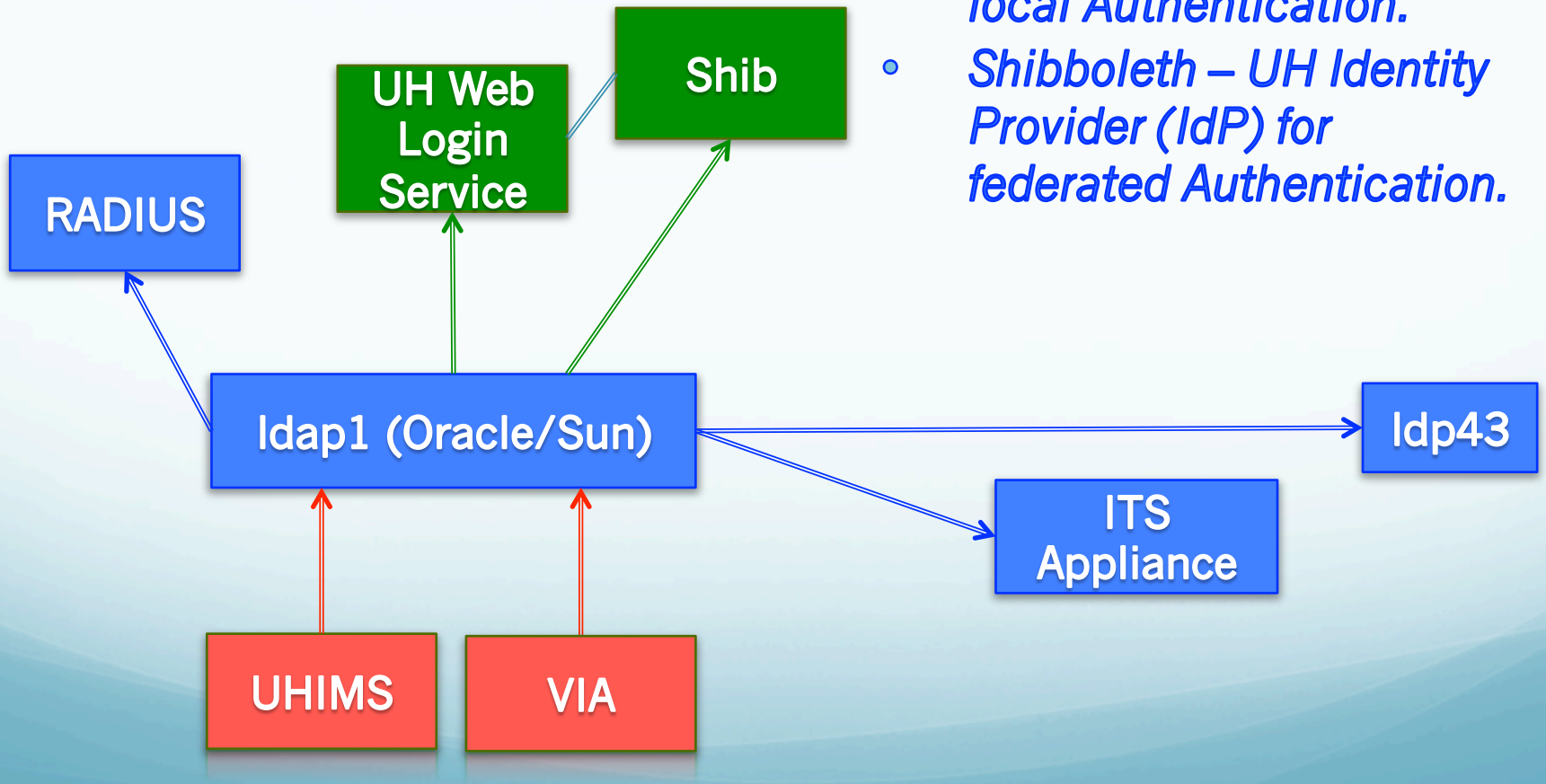
- VIA – adds transient Visitor accounts to LDAP
- UHIMS – adds anyone associated with UH to LDAP



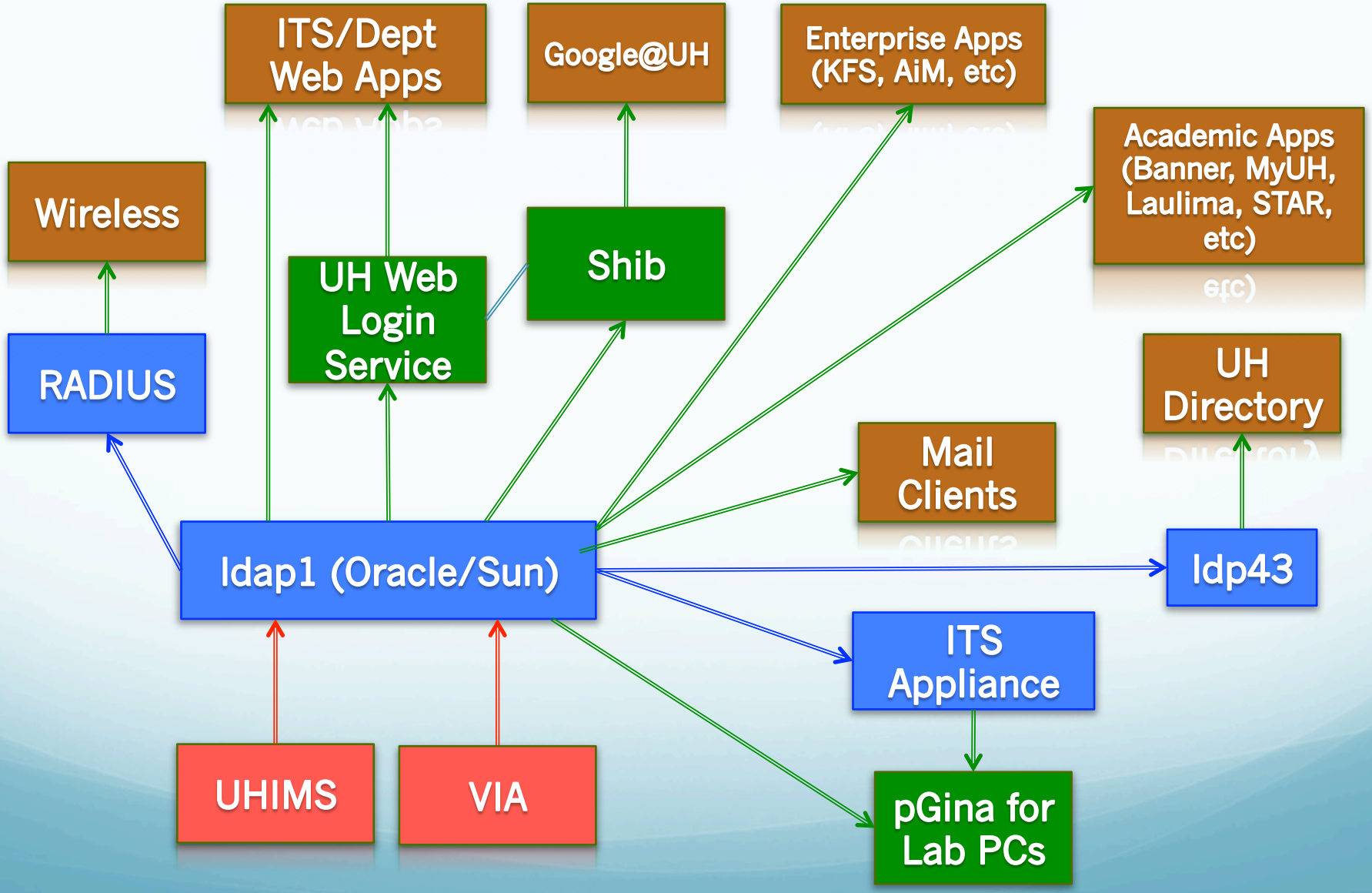
LDAP for AuthN Today

Centralized Authentication Components

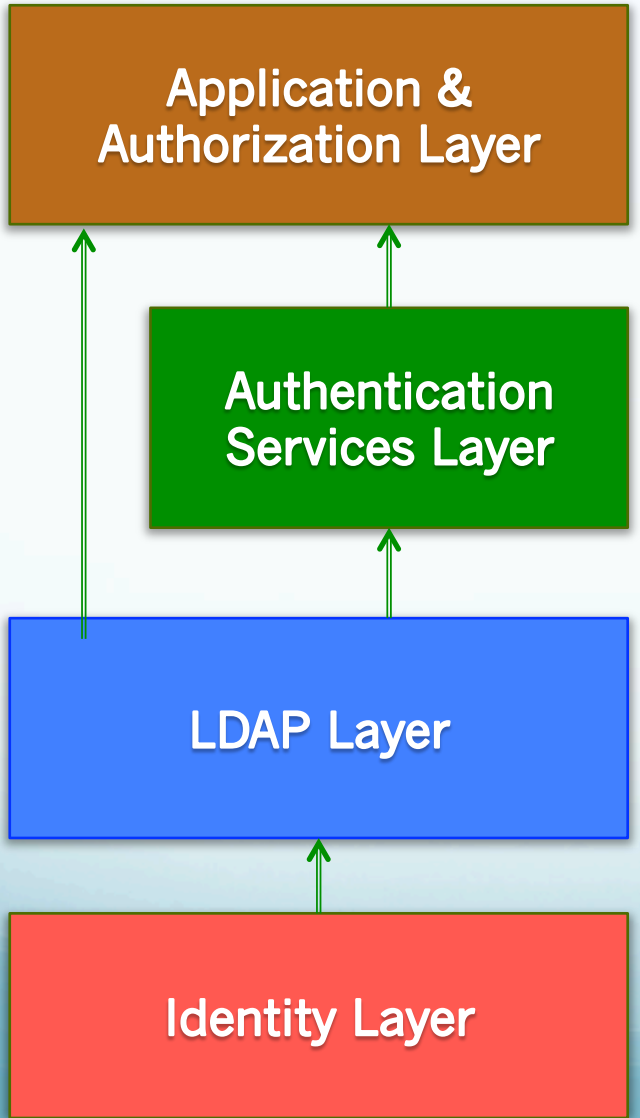
- *UH Web Login Service for local Authentication.*
- *Shibboleth – UH Identity Provider (IdP) for federated Authentication.*

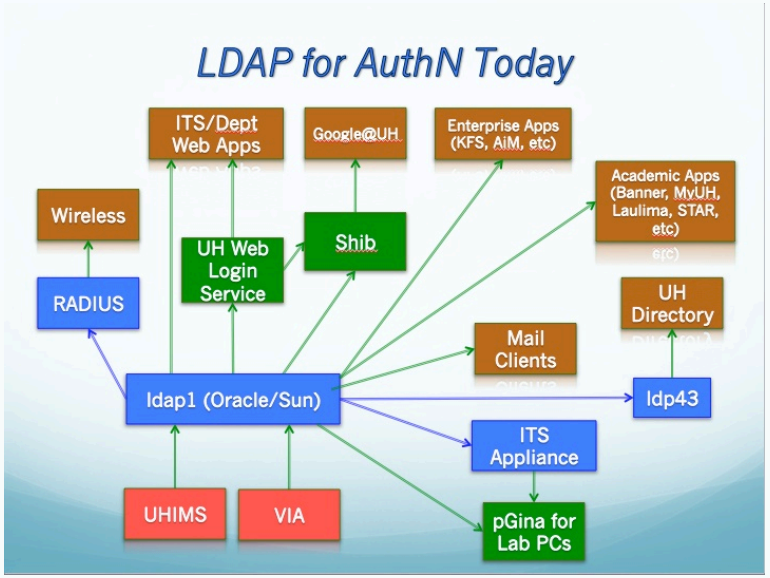


LDAP for AuthN Today



LDAP for AuthN Today

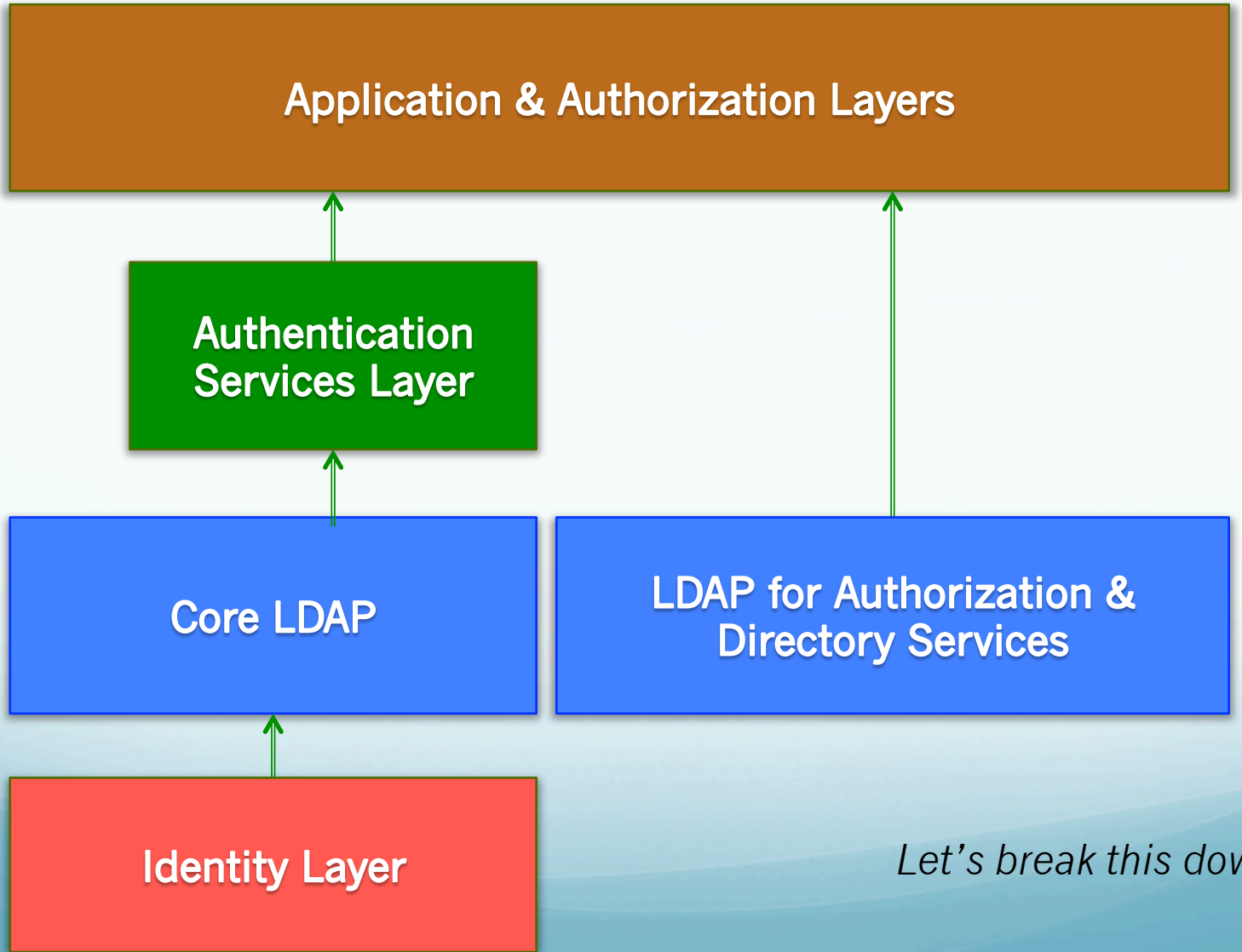




LIMITATIONS:

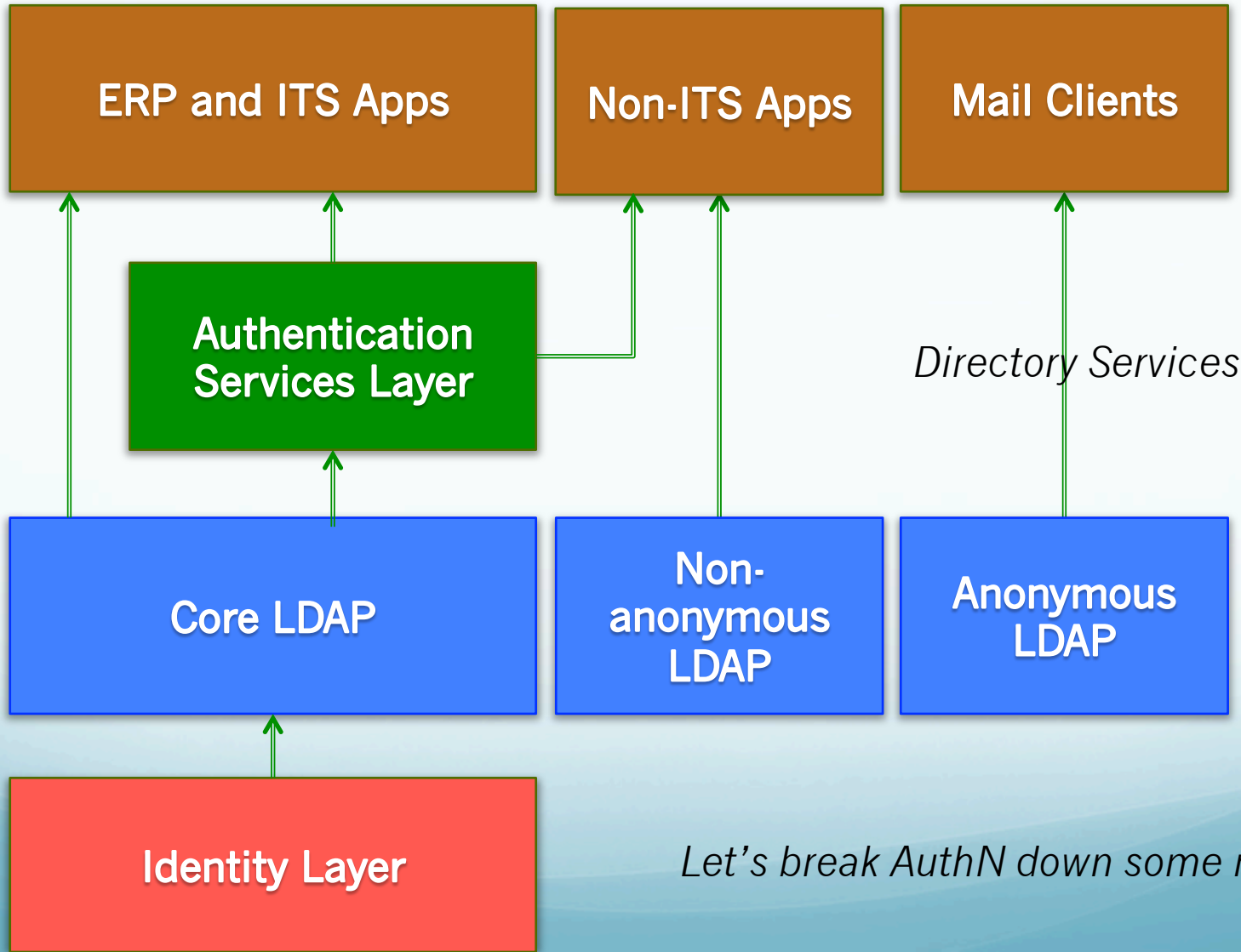
- *Subject to performance issues.*
- *Doesn't isolate core AuthN and Directory Services.*
- *Doesn't allow for additional fine-tuning of security.*

LDAP for AuthN Tomorrow



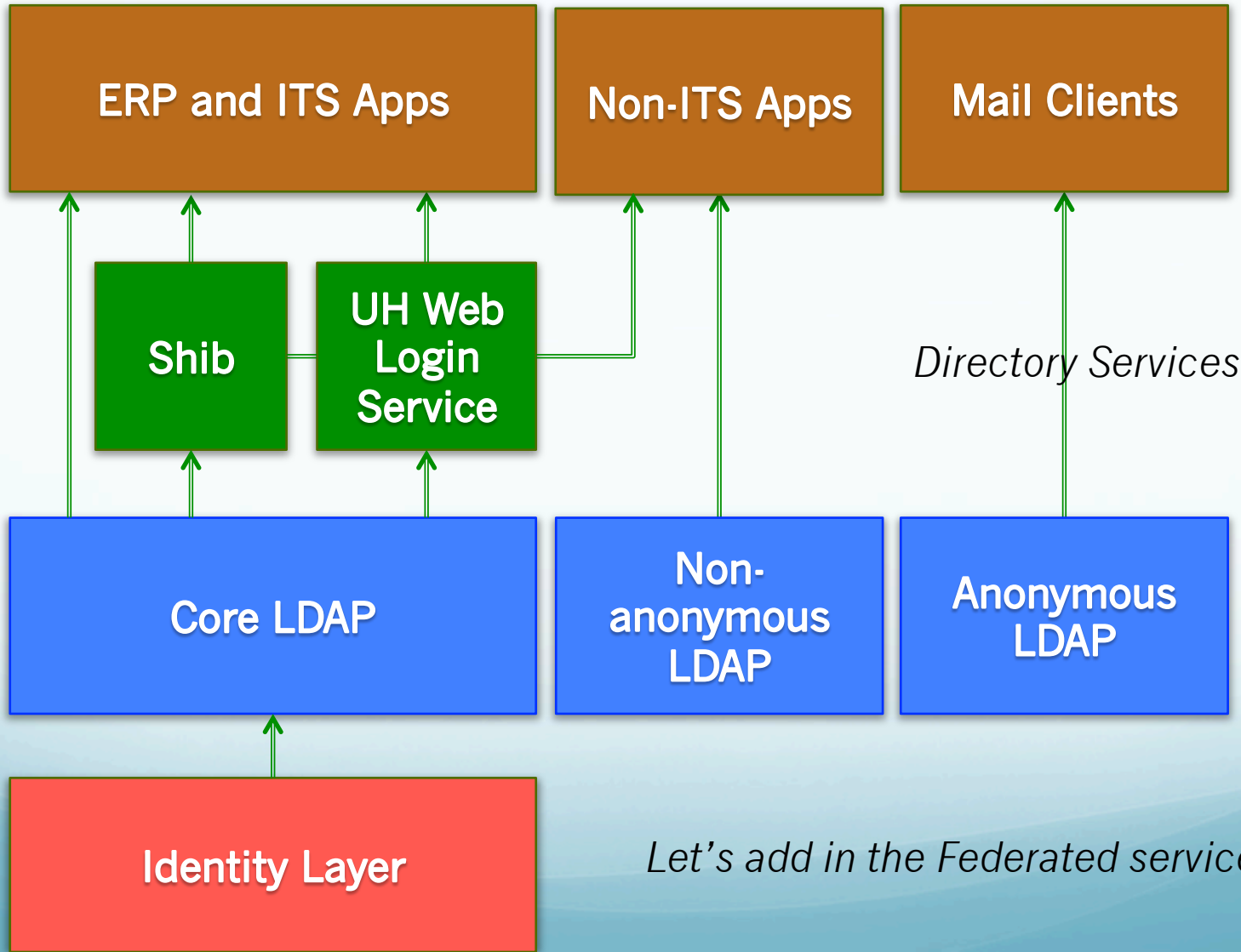
Let's break this down . . .

LDAP for AuthN Tomorrow



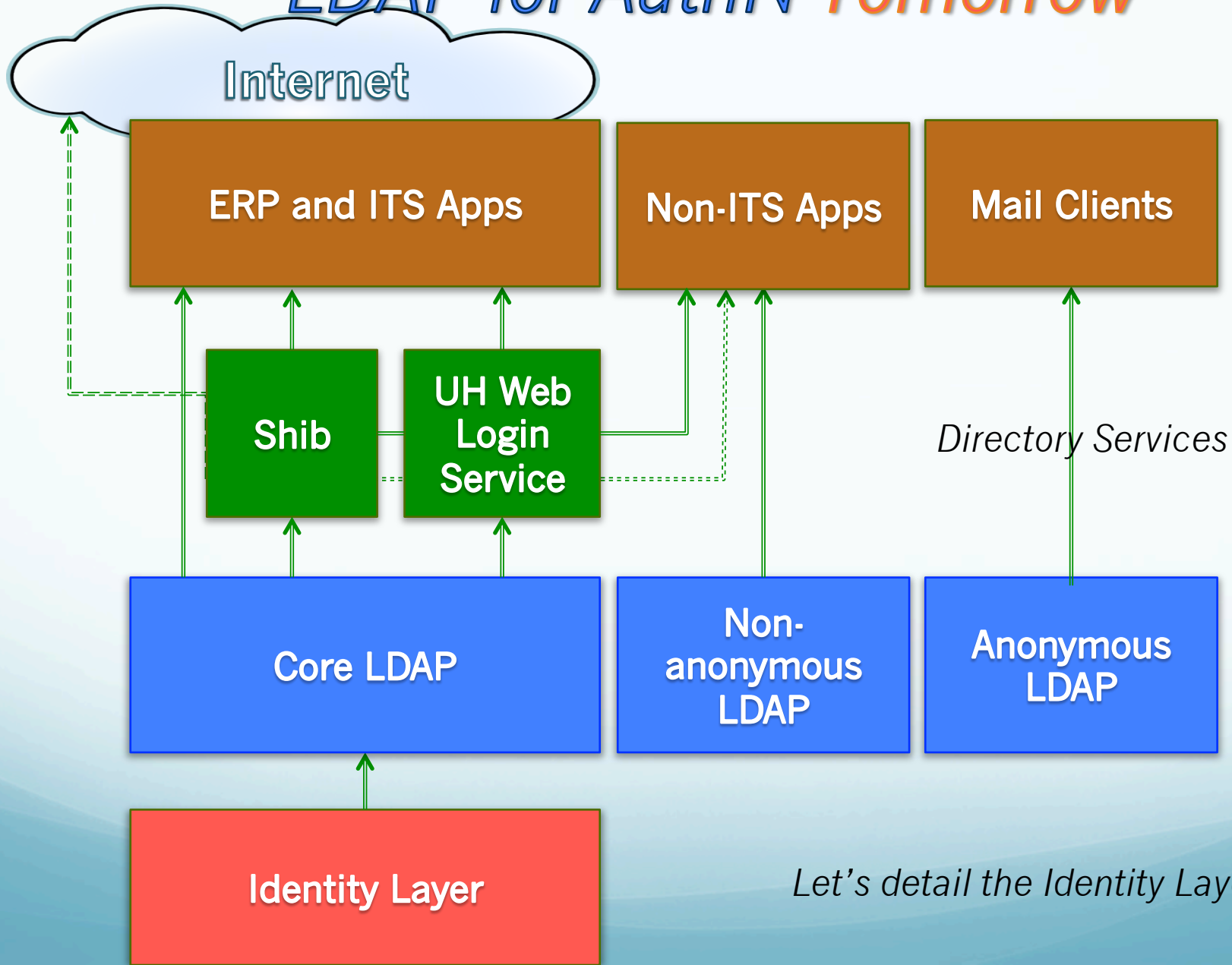
Let's break AuthN down some more . . .

LDAP for AuthN Tomorrow



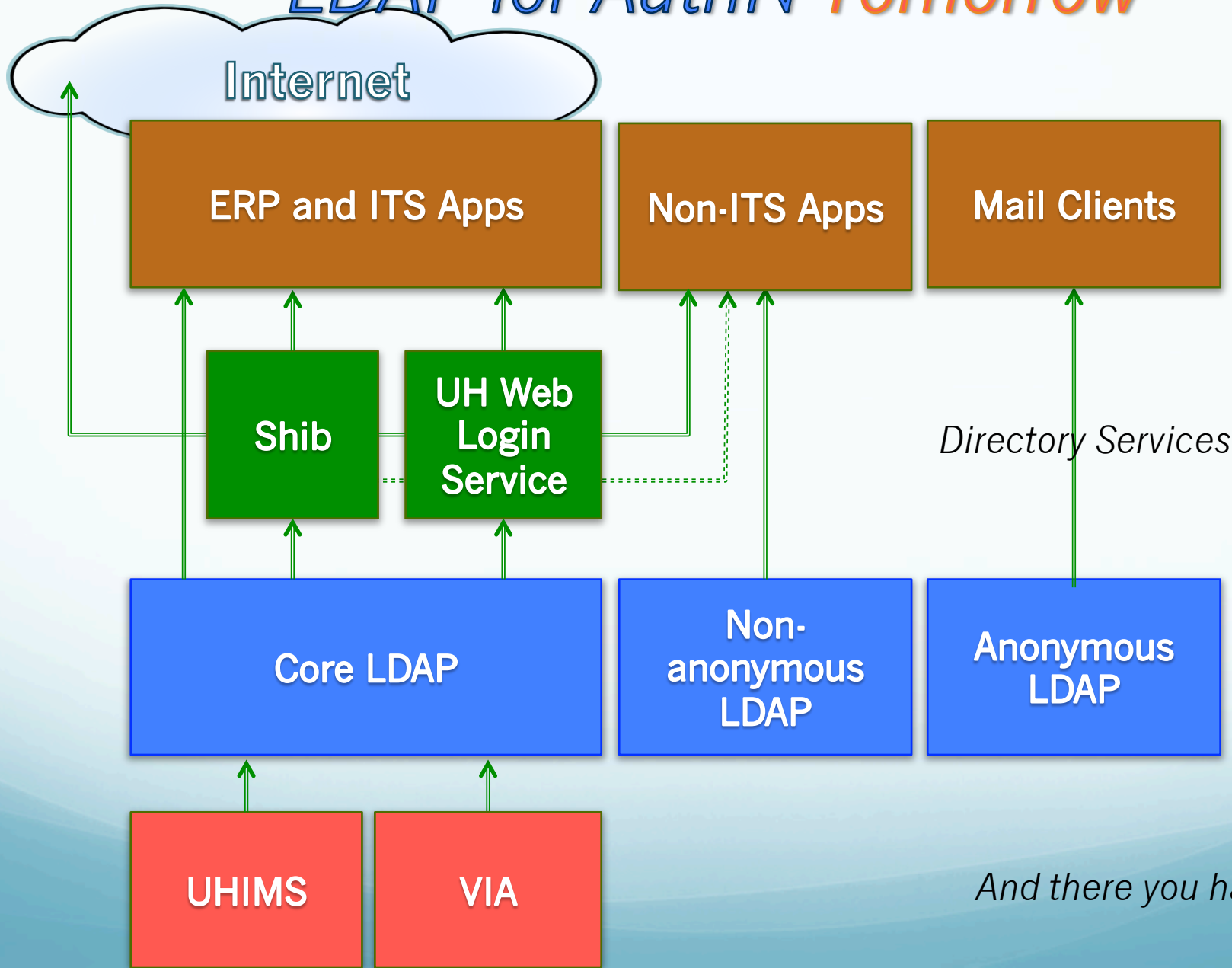
Let's add in the Federated services . . .

LDAP for AuthN Tomorrow



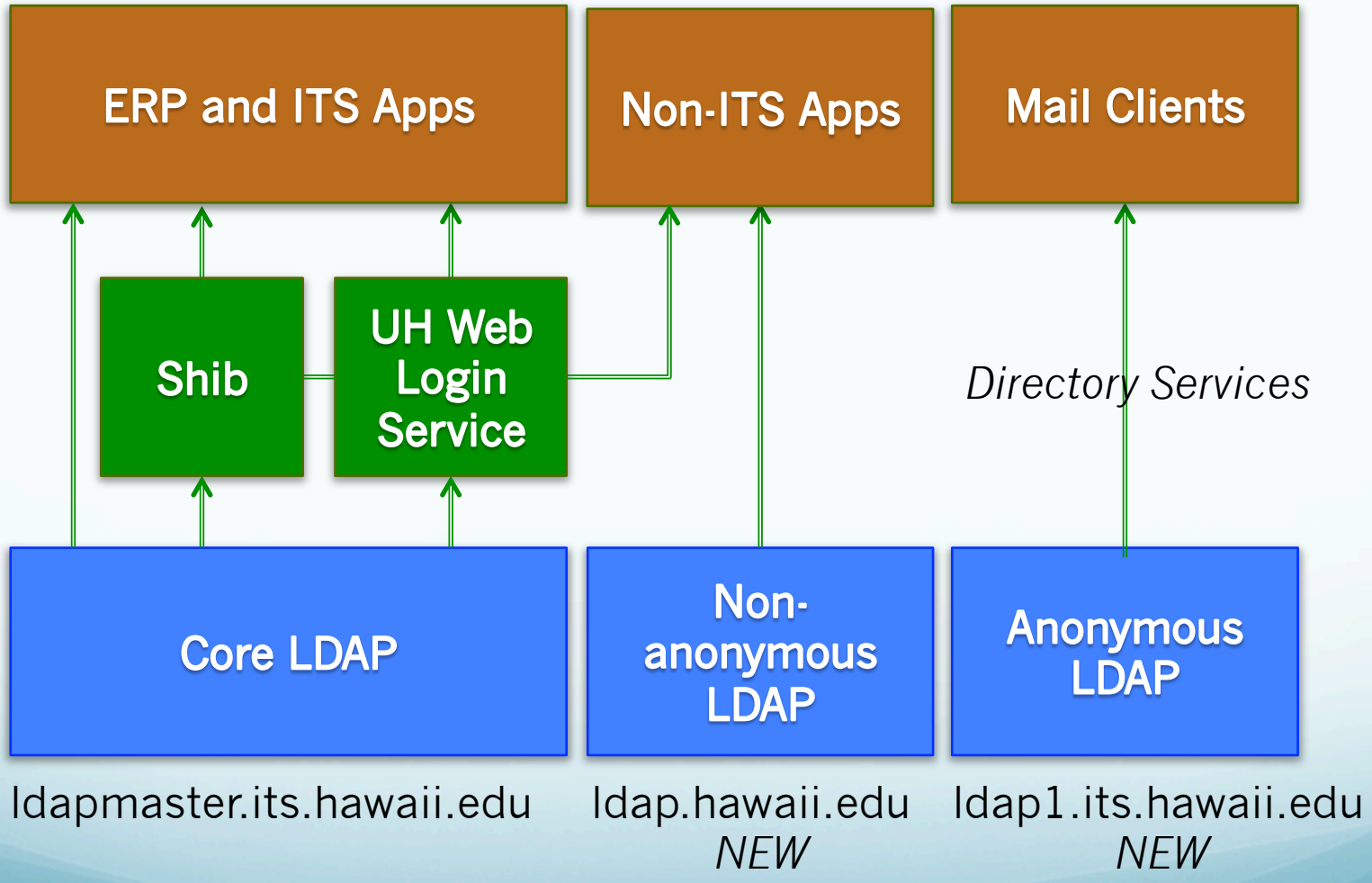
Let's detail the Identity Layer . . .

LDAP for AuthN Tomorrow

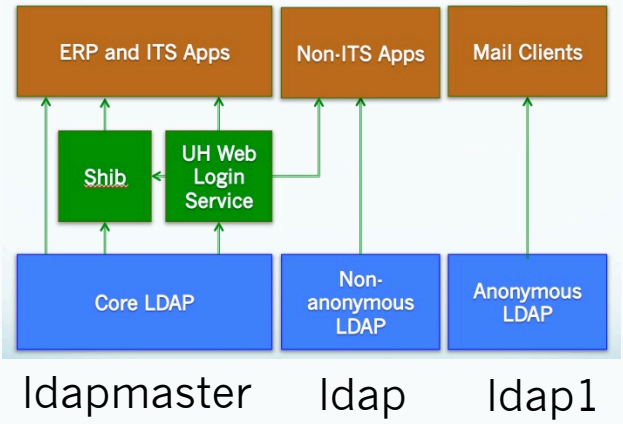


And there you have it.

LDAP for AuthN Tomorrow



LDAP for AuthN Tomorrow



- *ldap1 remains the same; many mail clients point to it.*
- *We will monitor ldap1 to determine which applications need to move to ldap.hawaii.edu and register.*
- *Eventually we would like to require mail clients to also authenticate against ldap1 so that we can disallow anonymous.*

- *ITS is also replacing Oracle Enterprise LDAP servers with 389ds open-source servers; ldapmaster will be first.*
- *UH developers will have time, but need to plan for migrating LDAP references to ldap.hawaii.edu.*
- *UH developers will be provided with a test LDAP environment; date to be determined.*

LDAP for AuthN Tomorrow

Questions?

Disclaimer: “tomorrow” is not meant to be taken literally in these slides.

UH Applications Developers 2/10/2012

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

Thank you!!!