# Lanka Education and Research Network

# Introduction to Identity Access Management

## IAM in Campus Networks

26th September 2018

*Workshop on Federated Identity Management*

LEARN

Based on APAN-Backfire / Tuakiri / AAF / SWITCH / IDEM content on IAM

# Design Goals for Identity and R&E

- Stone Age
  Application maintains unique credential and identity information for each user locally
- Bronze Age
  Credentials are centralized (e.g. Kerberos, LDAP) but applications maintain all user identity information
- Iron Age
  Credentials and core identity information is centralized and application maintains only app-specific user data

# Design Goals for Identity and R&E

***The Dream*** - providing users with a single login that grants access to any resource, irrespective of device or physical location.

When designing for Identity Management (IdM) start with your desired end goals and then work backwards.

- Single Sign On (SSO)
- Role-based access to network resources
- Support for traveling scholars (think “eduroam”)
- Tools for collaboration
- Shared access to remote instruments
- *Your wish list goes here*

# Why Focus on Campus Networks?

- Individual institutions are the authoritative source for domain data
- The campus network is the foundation for research and education activities
- The best path to network capacity, equipment and personnel
- No researcher is connected directly to a national R&E network
  - They are all connected to campus or enterprise networks for access

# Benefits for Campus Network Operators

When staff and money are in short supply, any new effort must add value to entire campus plan. IdM can provide:

- better utilization data
- better security
- better management for restricted resources

These things come at a cost as there are new services and software to manage and someone will have to maintain data integrity on an on-going basis.

*The value goes beyond IdM.*

# The Model

Centered on the User Identifier (NetID) - A single unique University wide identifier bound to the individual user and used at log-in to provision:

- Authentication
  - Quickly verify user identities (Who you are)
- Authorization
  - Control users access (What you can access)
- Administration
  - Manage user privileges by role, group, status, etc.
  - Allows for fine-grained policy application

# Communities of Practice

The R&E community has several well developed forums for Identity practitioners which are open to new participants. These forums include training resources, special advanced topic working groups, and documentation on current best practices. The sites provide both technical and policy guidance.

- REFEDS (Research and Education FEDerations group)
  - EU-based group https://refeds.org/
- InCommon(operated by Internet2 Staff)
  - US/Internet2 Based group https://www.incommon.org/
- eduroam (education roaming)
  - secure, world-wide roaming access service
  - https://www.eduroam.org/
- eduGAIN (operated by GÉANT)
  - interconnects identity federations around the world
  - http://www.eduGAIN.org/

# Campus Identity Systems evolution

## Campus IAM

## Identities

- Registries of who/what, identifiers, attributes, systems integration

## Credentials & authentication

- Internal, external
- Linked to Identity

## Access management

- Roles, rules, entitlement, affiliation, groups, privileges, policy, authority, delegation, etc.

# Factors to Consider in IAM Platforms

## Variable distance from the data

- Local - Systems of Record, home grown, commercial
  - Internally, apps enjoy tightly coupled access to fresh data
  - Usually ‘behind the wall’
- Federated – apps aware of more than local & remote systems of record
  - accept other identities underpinned by a trust decision
  - Foot in both worlds at times -- inside & outside the wall.
  - Data ‘distance’ further out
    - Upon sign-in of user, or provisioning task
- Cloud (aka SaaS, PaaS) - apps abstracted away lower level details, could be furthest away from your fresh data
  - Similar challenges as federated
  - SLAs may or may not be under your control
  - Outside the wall
  - Deployment profile & app sophistication guide data management

# Factors: Governance and Process

## Governance

- Clarity around:
  - Who says who says
  - Authorization model:
    - Centralized or distributed?
    - Application or data centric?

## Process and Practices

- Are change control practices in place & recognize the implications of local, federated, and cloud use styles?
- System Of Record steward may not realize:
  - Dependencies on their data and change turnaround
  - How far flung systems of record data may be

# The Evolution of Access Management

| Phase | Description |
|---|---|
| None – most physical controls | If you can authenticate, you get everything |
| Control by contract | If you can authenticate, you get everything, but there is no abuse policy in place |
| Hard coded privilege tables at the resource | Authorization at the application level |
| The above + LDAP calls for intrinsic attributes | Authorization starts to depend on external attributes |
| An attribute authority | An application or service can get any attribute that the access management policies permit |
| An external yes/no authorization service | An external service calculates whether access is permitted |

# Federated Identity

- Current mechanisms assume applications are within the same administrative domain
  - Adding an external user means creating an account in your ID system. This could result in the new user having access to more than just the intended application.
- Federated Identity Management (FIM) securely shares information managed at a users home organization with remote services.
  - Within FIM systems it doesn't matter if the service is in your administrative domain or another. It's all handled the same.

# Federated Identity

In Federated Identity Management:

- **Authentication** (AuthN) takes place where the user is known
- An **Identity Provider** (IdP) publishes authentication and identity information about its users
- **Authorization** (AuthZ) happens on the service's side
- A **Service Provider** (SP) relies on the AuthN at the IdP, consumes the information the IdP provided and makes it available to the application
- An **entity** is a generic term for IdP or SP

The first principle within federated identity management is the active protection of user information

- Protect the user’s credentials
- only the IdP ever handles the credentials
- Protect the user's personal data, including the identifier
- a customized set of information gets released to each SP

# Identity Providers

Organisations with users run Identity Providers

- Provide a login page
- Provides a mechanism for consent of attribute release
- Login page is branded to the organisation
- Login against the organisation LDAP or AD
- Manages password reset
- Provisions and de-provisions accounts
- Agrees to the federation policies

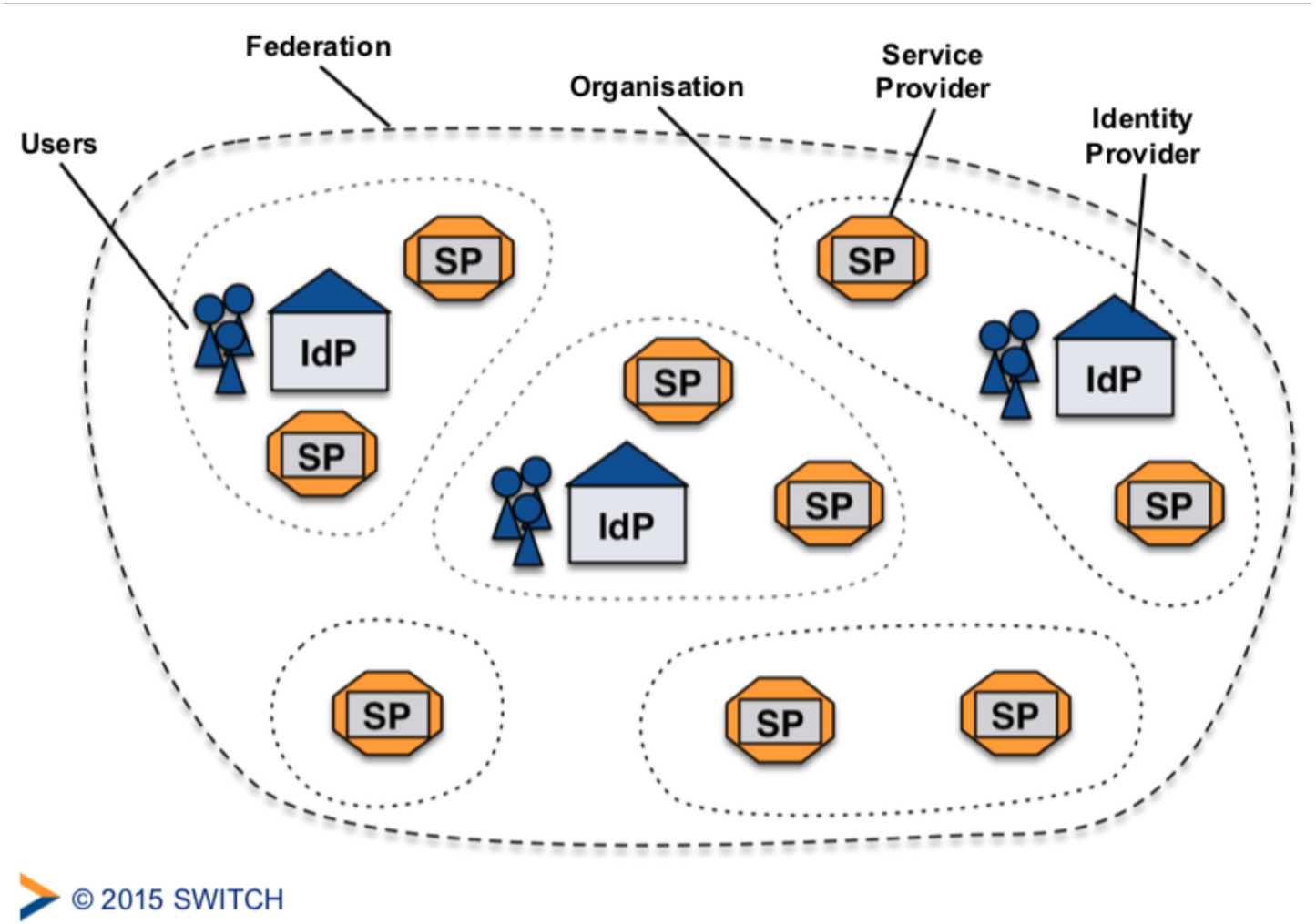
Can be used for campus Single Sign-on as well as federated SSO!

# Service Providers

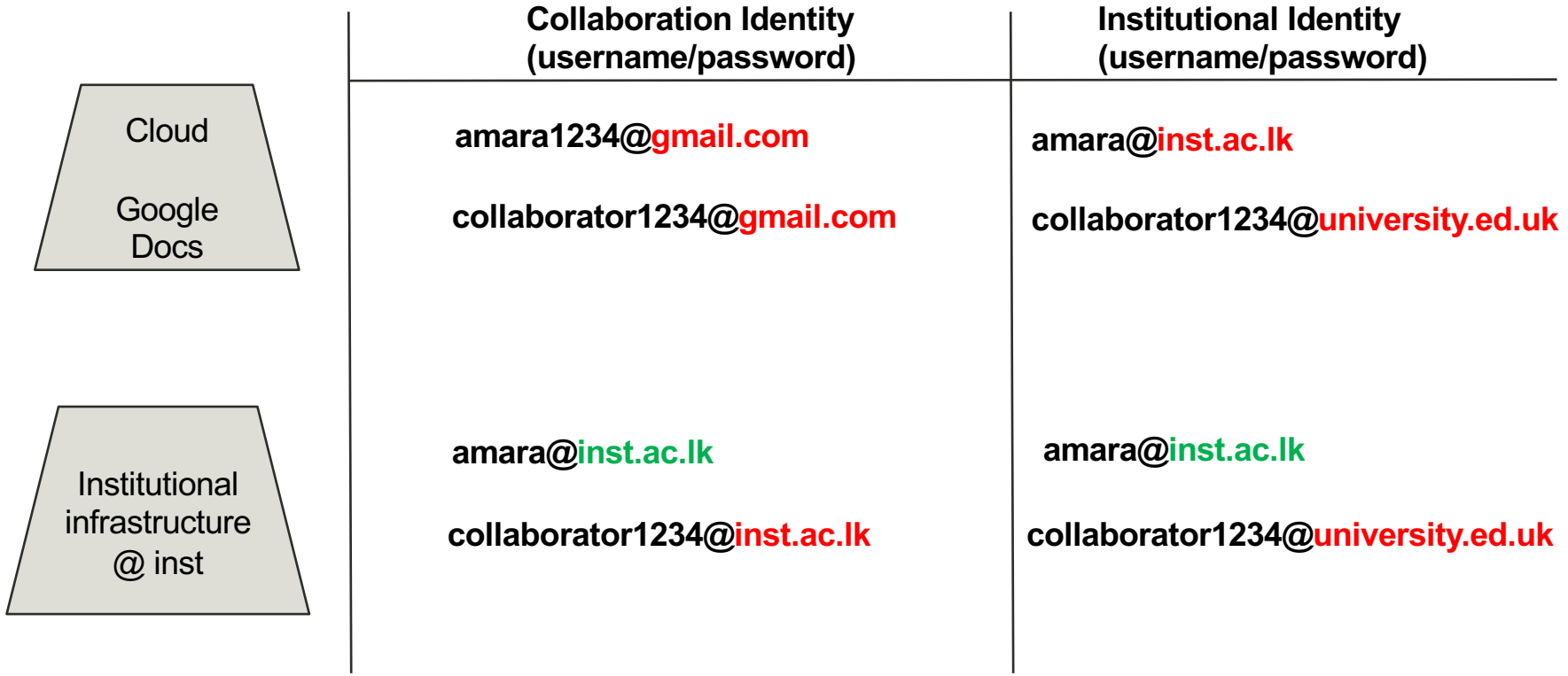
Run by organizations that have something to offer the federation community

- Hands off authentication to IdPs
- Obtains attributes from IdPs
- Agrees to the federation policies

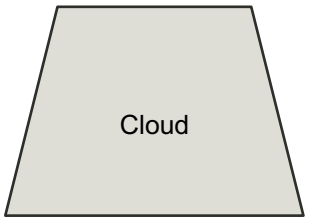
# Federated Identity Management

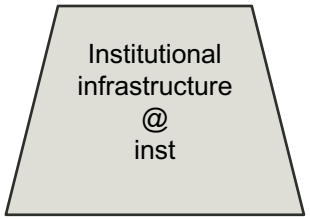


# Traditional Approach



# FIM Approach




| | Collaboration Identity (username/password) | Institutional Identity (username/password) |
|---|---|---|
| Cloud | amara@inst.ac.lk | amara@inst.ac.lk |
| | collaborator1234@university.ed.uk | collaborator1234@university.ed.uk |
| Institutional infrastructure @ inst | amara@inst.ac.lk | amara@inst.ac.lk |
| | collaborator1234@university.ed.uk | collaborator1234@university.ed.uk |

# Why not Google, Facebook, Yahoo!, Twitter..?

Interfederation Research Participants (eduGAIN *via* InCommon, Canarie, etc.) are responsible for investigating and compliance with international privacy law of the countries where research occurs or research subjects reside - *Susan Blair, Chief Privacy Officer, University of Florida, Internet2 Global Summit 2015*

- Google Policy: “Information we collect when you are **signed into Google**, in addition to information we obtain about you from partners, may be associated with your Google Account. When information is associated with your Google Account, we treat it as personal information.”

# Benefits of Federated Identity Management

- Reduces work
  - Authentication-related calls to Penn State University's helpdesk dropped by 85% after they installed Shibboleth
- Provides current data
  - Studies of applications that maintain user data show that the majority of data is out of date. Are you "protecting" your app with stale data?
- Insulation from service compromises
  - With FIM data gets pushed to services as needed. An attacker can't get everyone's data on a compromised server.
- Minimize attack surface area
  - Only the IdP needs to be able to contact user data stores. All effort can be focused on securing this single connection instead of one (or more) connection per service.

# Benefits of Federated Identity Management

- Users generally find the resulting single sign-on experience to be nicer than logging in numerous times.
- Usability-focused individuals like that the authentication process is consistent regardless of the service accessed.
- A properly maintained federation drastically simplifies the process of integrating new services.

# Benefits of Federated Identity Management

Increase Customer Base

- Opportunity of global research and education federations
- Benefits of inter-federation via eduGAIN
- Opt-in to have your data shared with other federations via eduGAIN
- Service available in multiple nation federations across the globe

# Initial aims of FIM

- Simplify access to publisher content
- Support research activities
- Access global resources in eduGAIN
- Improve collaboration between organisations
- Reduce work load and support costs for your members
- Improve access for users
- Providing specific shared services (e.g. Library system)

# Questions

# Thank You

LEARN

Email: