

# ***FUTURE*** Directions

Identity and Access Management at UofT

# Overview

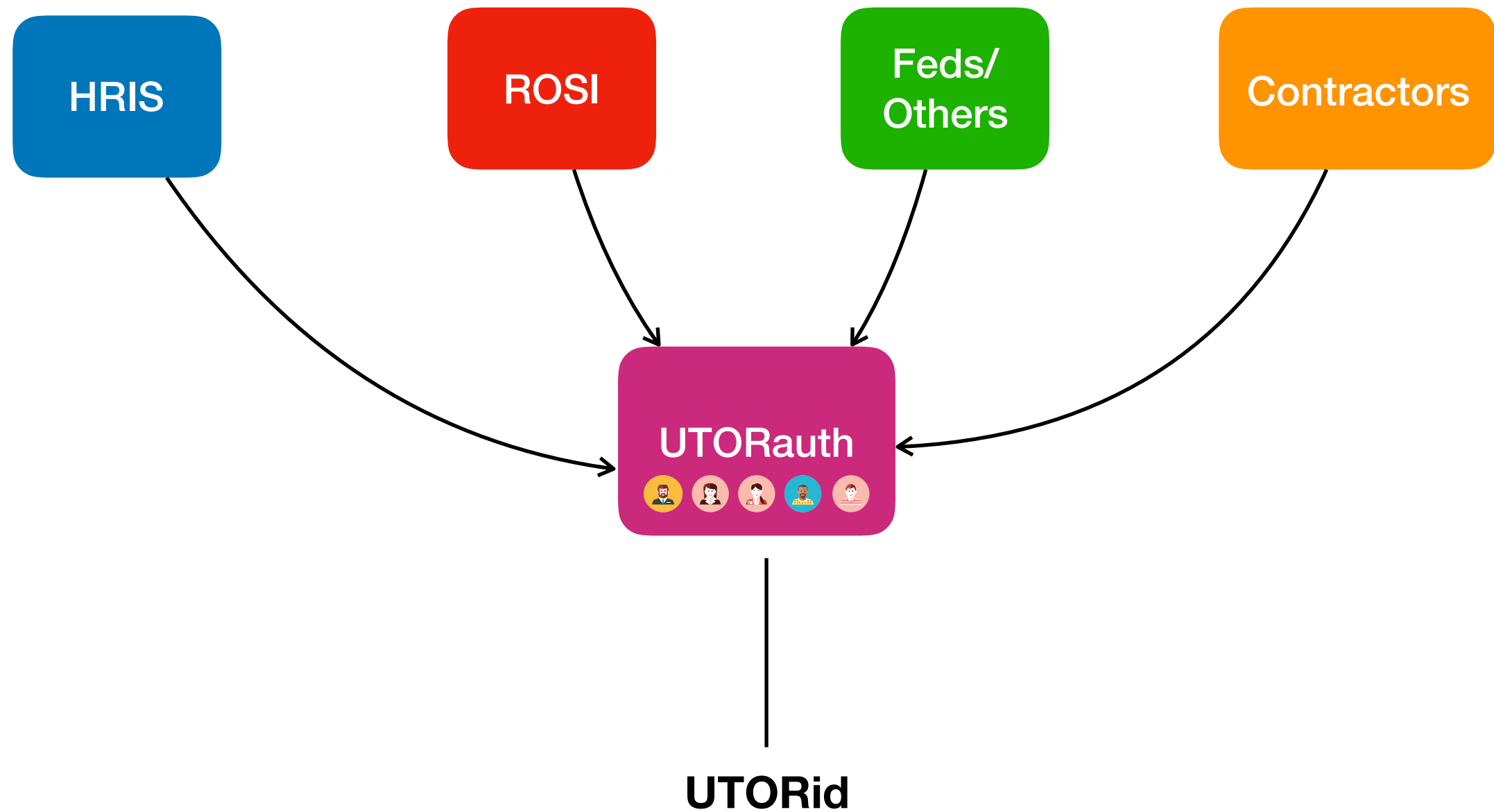
- Account Provisioning
- Group Management
- Guest Accounts

# Account Provisioning

# There was an idea...

- UTORauth: let's create a link between Systems of Record

# Account Provisioning











# There was an idea...

- UTORauth: let's create a link between Systems of Record
- Hard to do: differences in names cause duplication

# Duplication

This is the  
same guy!

UTORauth		
	Joe Smith	1984-06-08
	Joe Smith	1984-06-08
	Jane Doe	1951-02-15
	Bob Plant	1969-01-12
	Robert Plant	1969-01-12

ROSI		
	Joe Smith	1984-06-08
	Jane Doe	1951-02-15
	Bob Plant	1969-01-12

HRIS		
	Joe Smith	1984-06-08
	Jane Doe	1951-02-15
	Robert Plant	1969-01-12

# Duplication

<b>Last Year</b>	1297 total 890 (68%) detected automatically 407 (31%) submitted manually
<b>Last 6 Months</b>	894 total 633 (70%) detected automatically 261 (29%) submitted manually
<b>Last 3 Months</b>	436 total 280 (64%) detected automatically 156 (35%) submitted manually
<b>Last Month</b>	181 total 97 (53%) detected automatically 84 (46%) submitted manually
<b>Last Week</b>	67 total 16 (23%) detected automatically 51 (76%) submitted manually



# Another idea...

What if we could ask the end user if they already had an account?

# Current Model

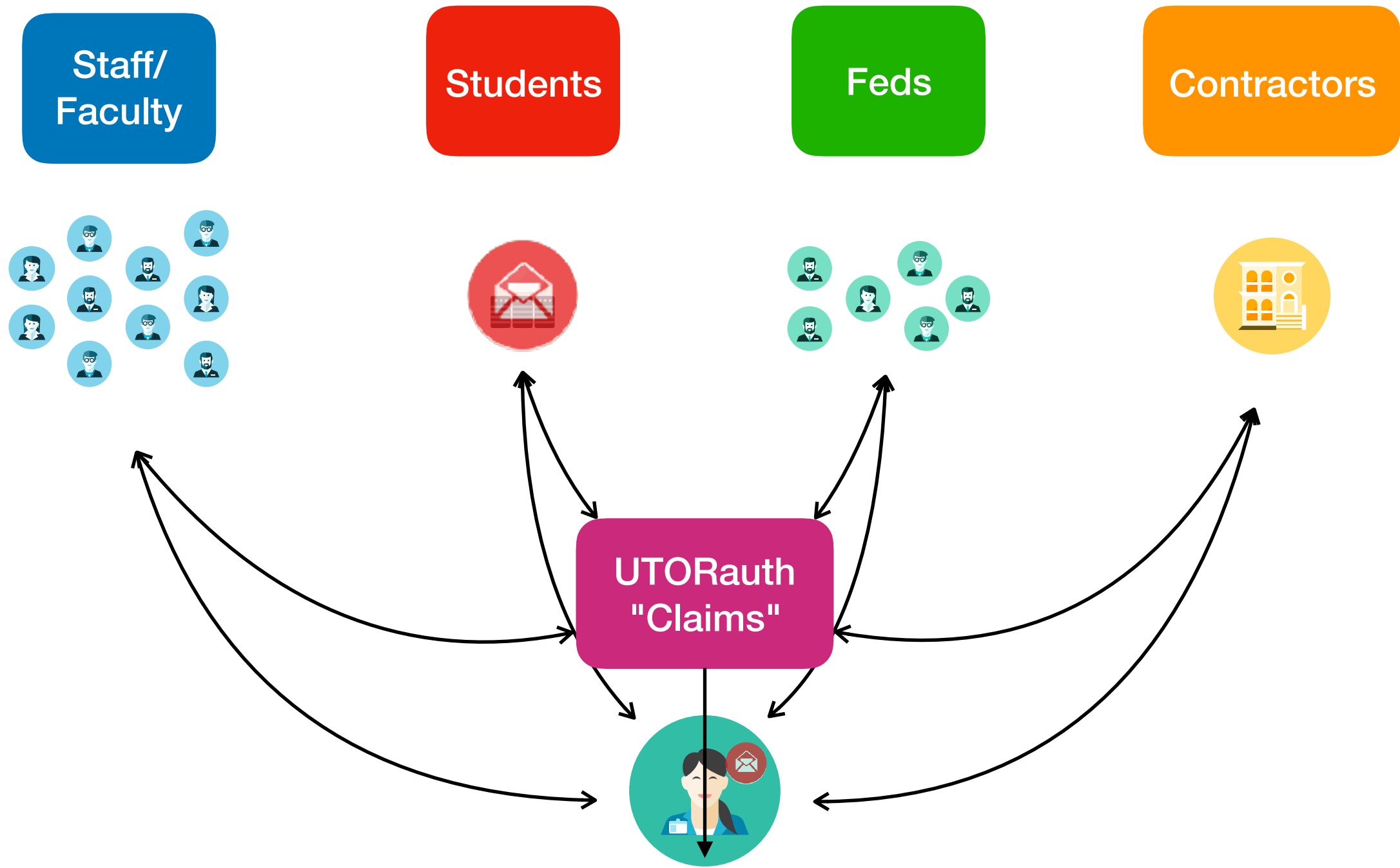
1. System of Record submits a person to UTORauth.
2. UTORauth searches for that person, either matches them to an existing UTORid, or creates a new one.
3. UTORid/JOINid sent to submitting system (sometimes real-time, sometimes batch).
4. Business officer / divisional email system, etc. communicates UTORid/JOINid and SAK via letter, email or phone call to client.

# "Claim" Model

1. System of Record requests an account, providing UTORauth with the client's external email address.
2. UTORauth emails the client a custom link to the "claim" website.
3. Website asks if client has an existing UTORid:
  1. If yes, client authenticates and proves they have one
  2. If no, a UTORid will be created.

# Benefits

- Reduction of the number of duplicate records
- Consolidation of end-user experience



# Benefits

- Reduction of the number of duplicate records
- Consolidation of end-user experience
- Remote users
- Guest accounts (more on this later)

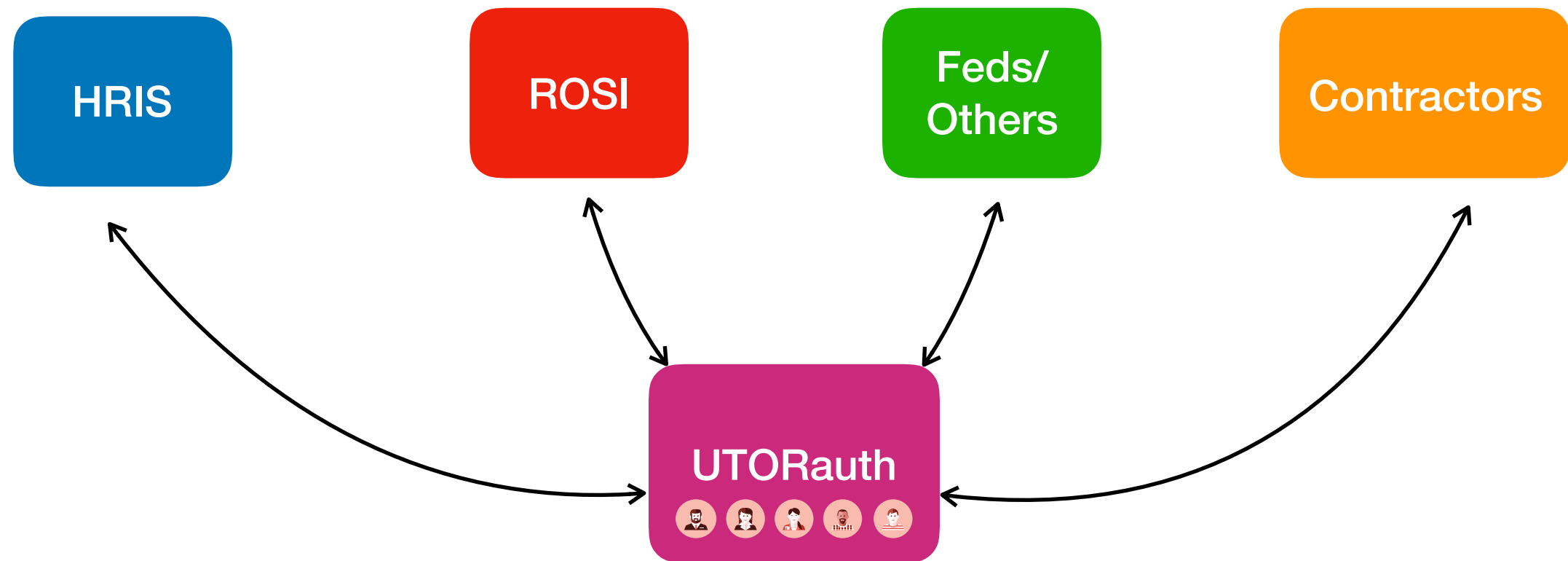
# Group Management

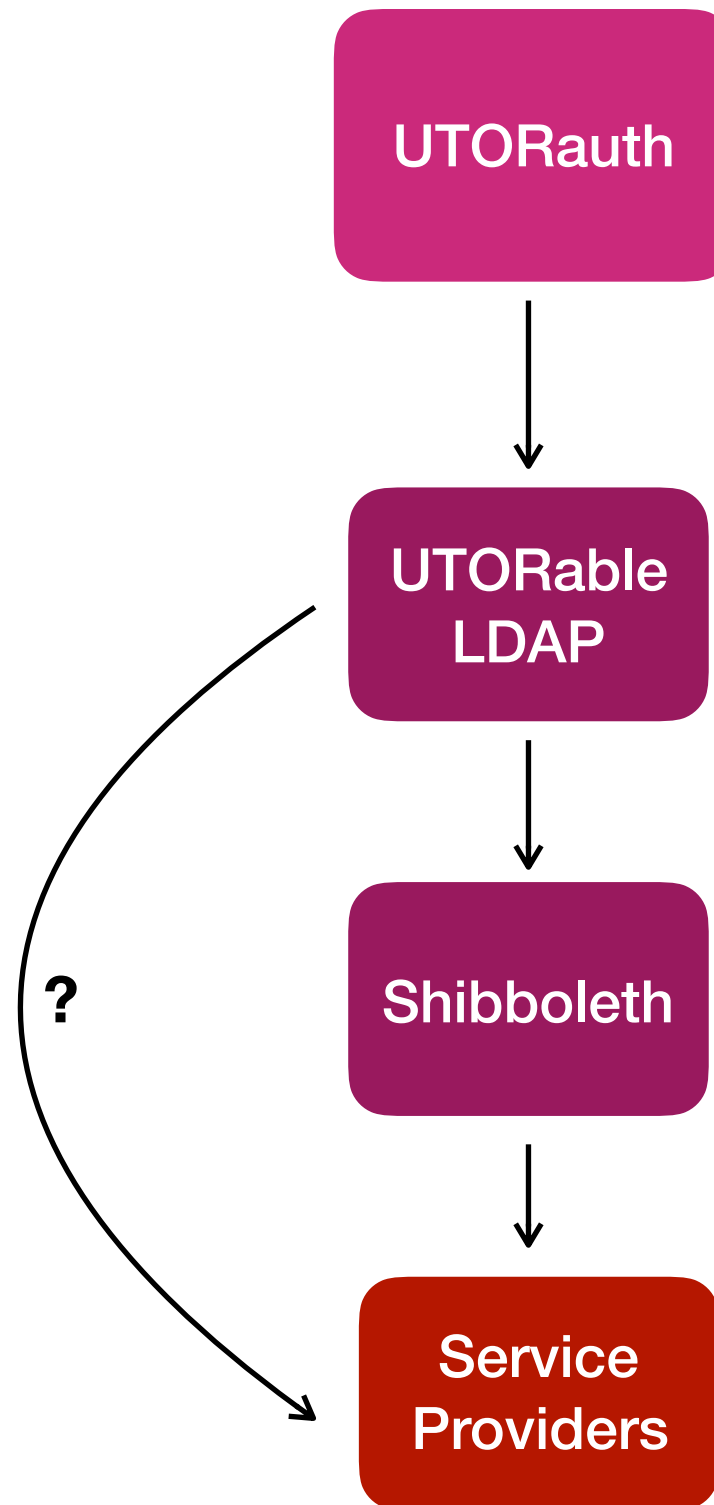
# Authorization

- UTORauth provides attributes, service providers make decisions
- UTORable LDAP contains coarse-grained information (isstaff, isfaculty, isstudent)



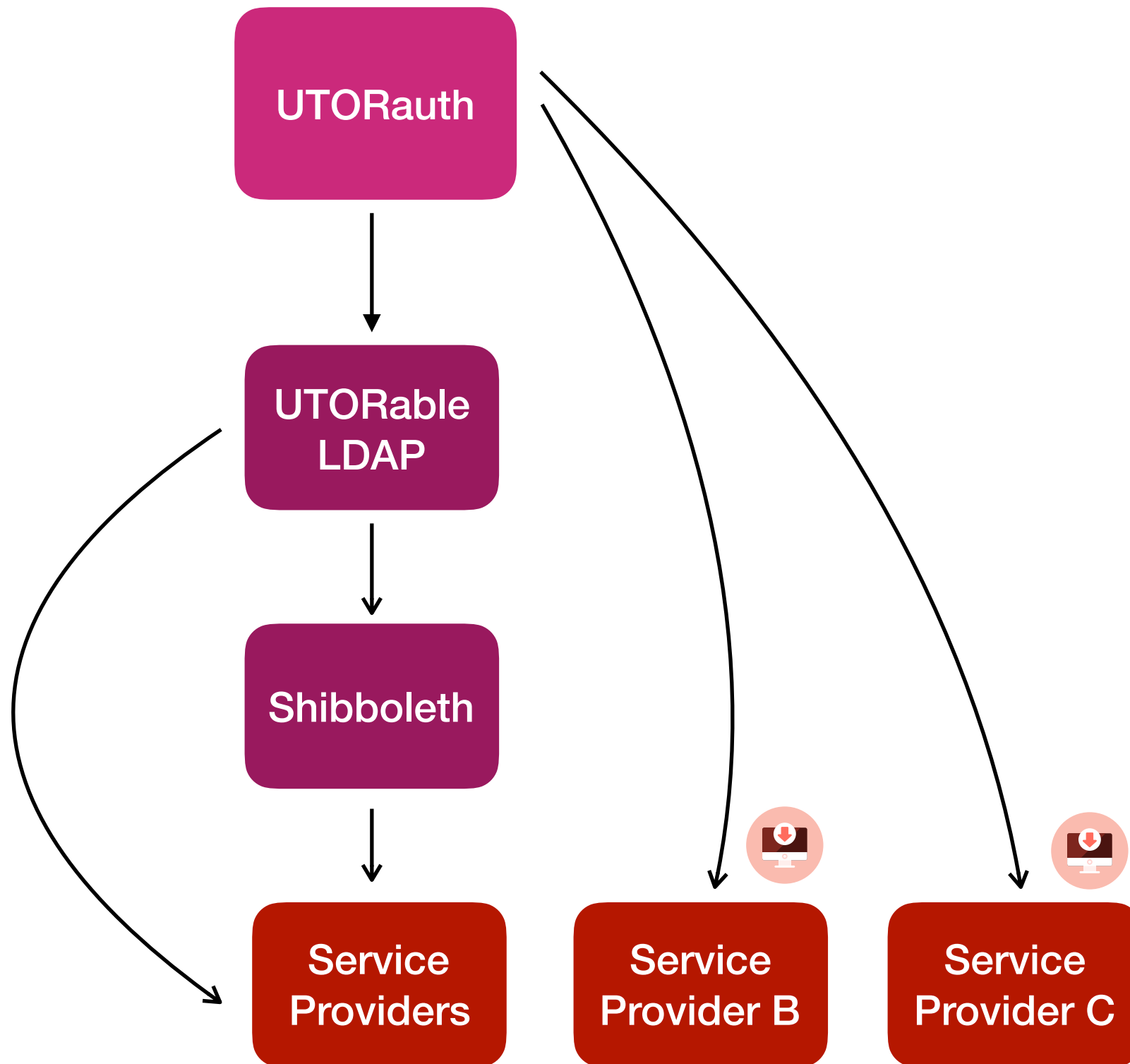
# Account Provisioning





# Challenges

- Service providers don't check
- Not enough information to make decisions -- batch feeds are created to fill the gap



# UTORGrouper to the rescue...

- Basis Groups: data driven
- Reference Groups: institutional cohorts
- Access Policy Groups: service provider maintained

# Basis Groups

- Driven by automated data
- Maintained and visible only to IAM staff
- Examples: Full-time staff, adjunct faculty, grad student, teaching hospital staff

# Reference Groups

- Constructed from basis groups
  - Staff Member = (full time staff + part time staff + federated college staff + ...)
  - Student = (grad student + undergrad student + continuing education student + ...)
- Maintained by IAM staff, but visible to service providers

# Access Policy Groups

- Constructed from reference groups and manually maintained allow/deny lists.
- Managed by the service provider
- An example...



# Example Access Policy

## Employee Services

Staff  
(reference  
group)

Faculty  
(reference  
group)

Allow  
List  
(manual  
group)

Deny  
List  
(manual  
group)

# Example 2.0

## Employee Services

Staff  
(reference  
group)

Faculty  
(reference  
group)

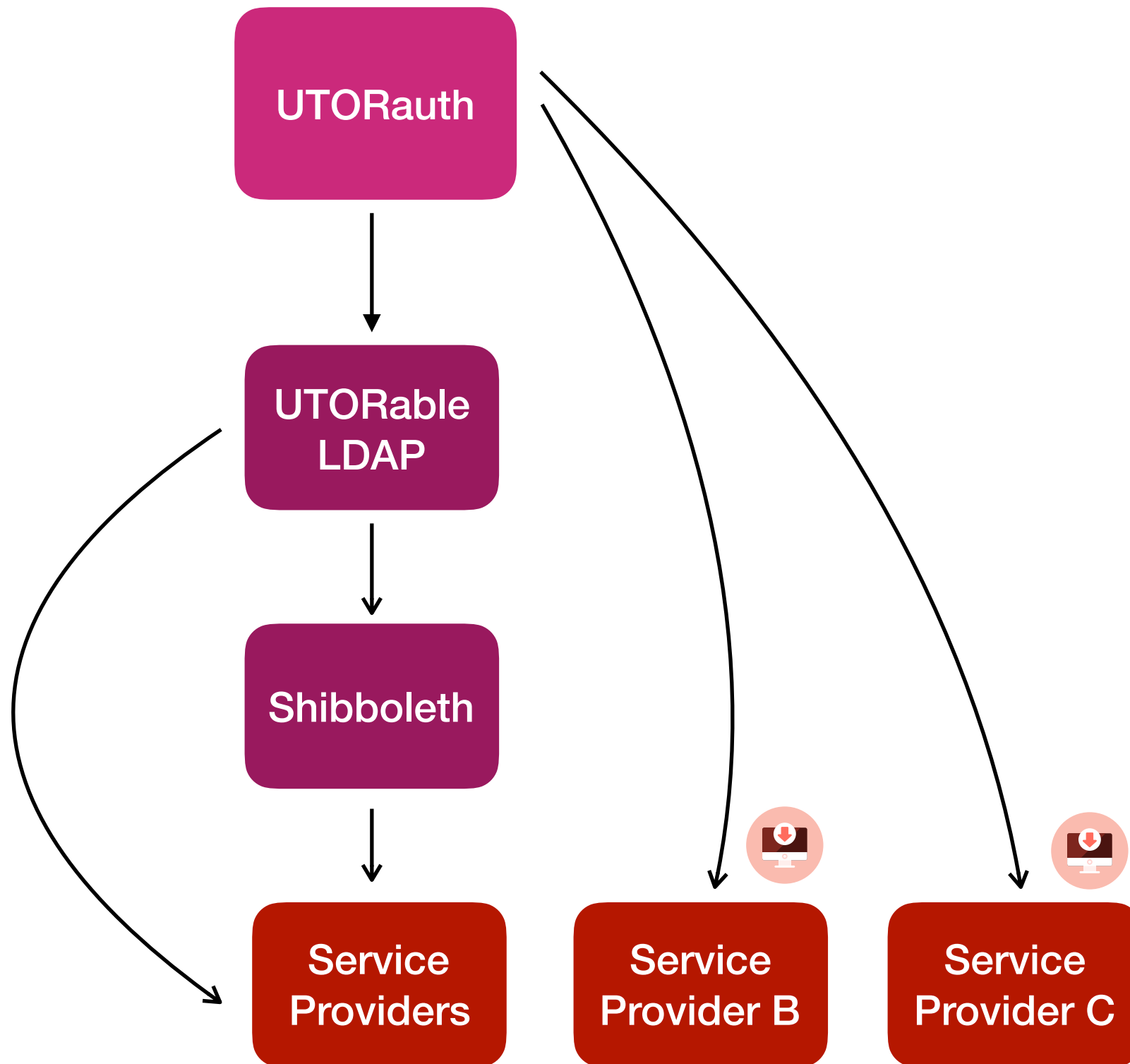
Allow  
List  
(manual  
group)

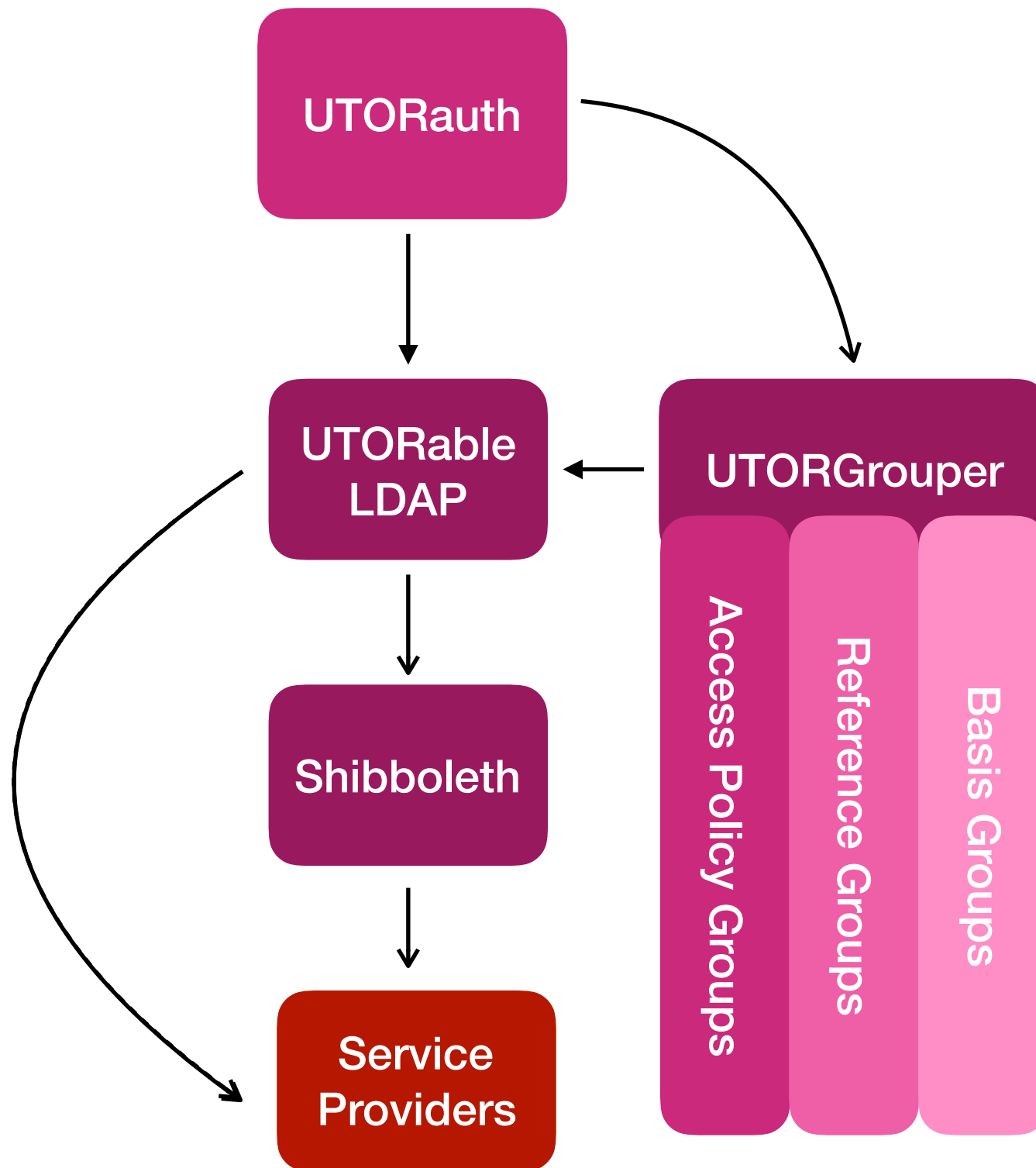
Deny  
List  
(manual  
group)

Blocked  
Accounts  
(ISEA  
maintained)

# Benefits

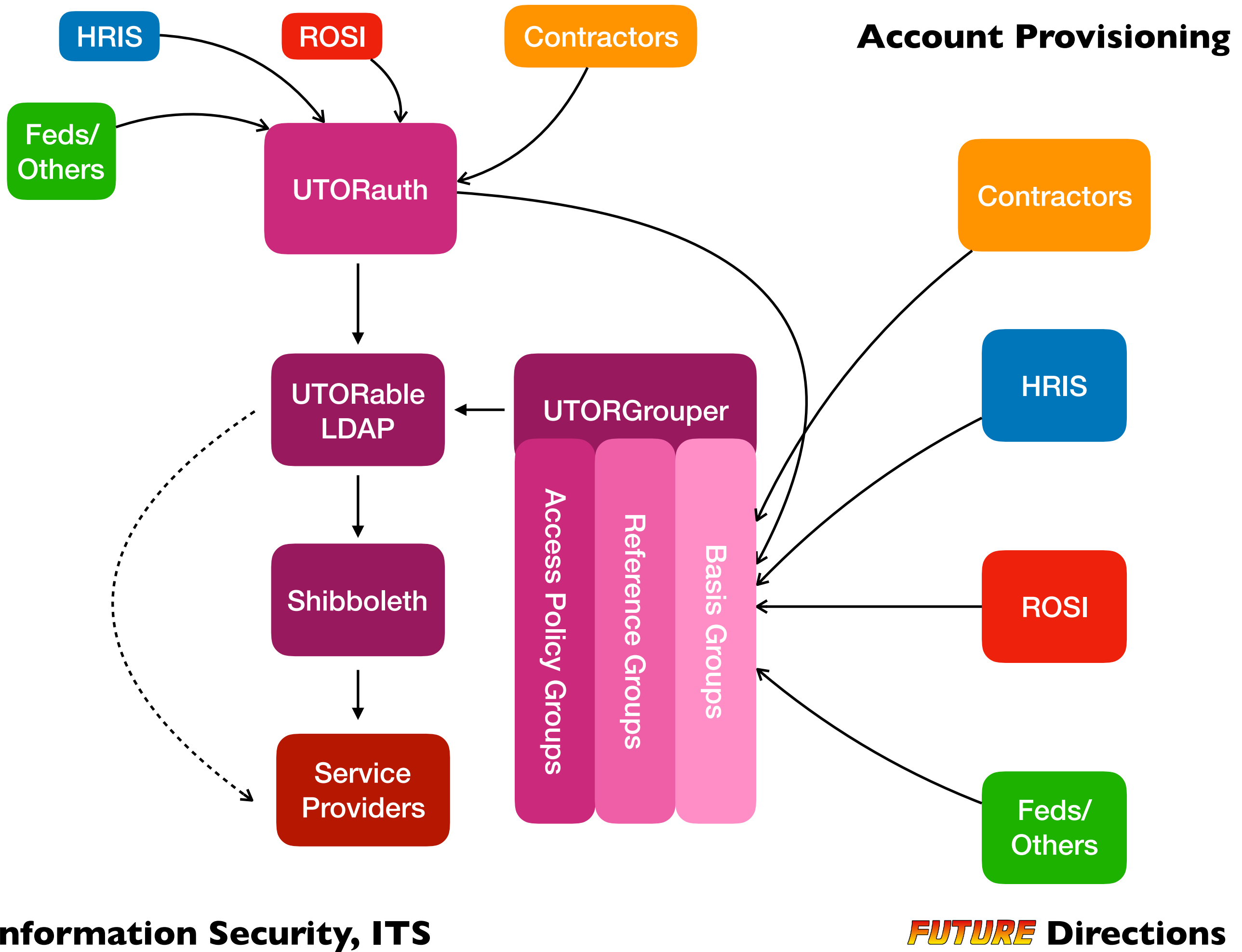
- Better control over who accesses your service





# Benefits

- Better control over who accesses your service
- Moving in the direction of near real-time updates to authorization



# Benefits

- Better control over who accesses your service
- Moving in the direction of near real-time updates to authorization
- Visibility into what services an account has
- Guest accounts



# Guest Accounts

# Currently...

- Guest access is fractured:
  - Long-term guest (contractor)
  - Short-term WiFi (QQ type 1)
  - Longer term Blackboard (QQ type 2)
  - etc...
- Apart from first type, not re-usable

# Claims + Groups = ...

- Proper guest account service
- Claims allows us to create named accounts for anyone (not QQ, not disposable)
- UTORGrouper allows us to provision temporary access to a service through allow/deny lists

# Questions?

[utorauth@utoronto.ca](mailto:utorauth@utoronto.ca)