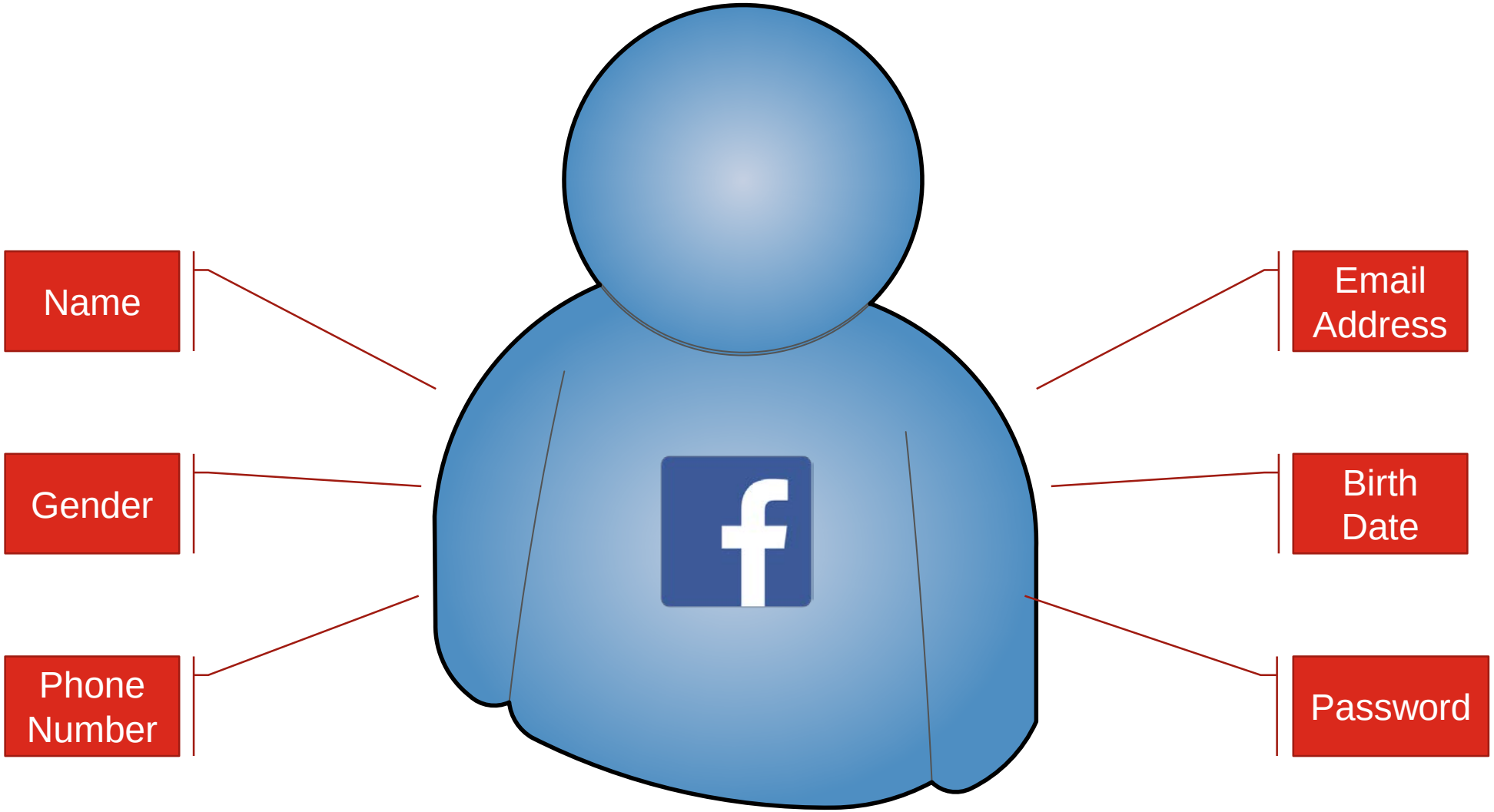
# *Identity & the Identity Management Lifecycle*

# *What is an Identity?*

ISO/IEC 24760-1 defines it as “a set of attributes related to an entity”

# *But then…what's an Entity ?*

- entity (n): a thing with distinct and independent existence
- We have lots of different types of entities in the identity space…


Name
Gender
Phone Number
Email Address
Birth Date
Password

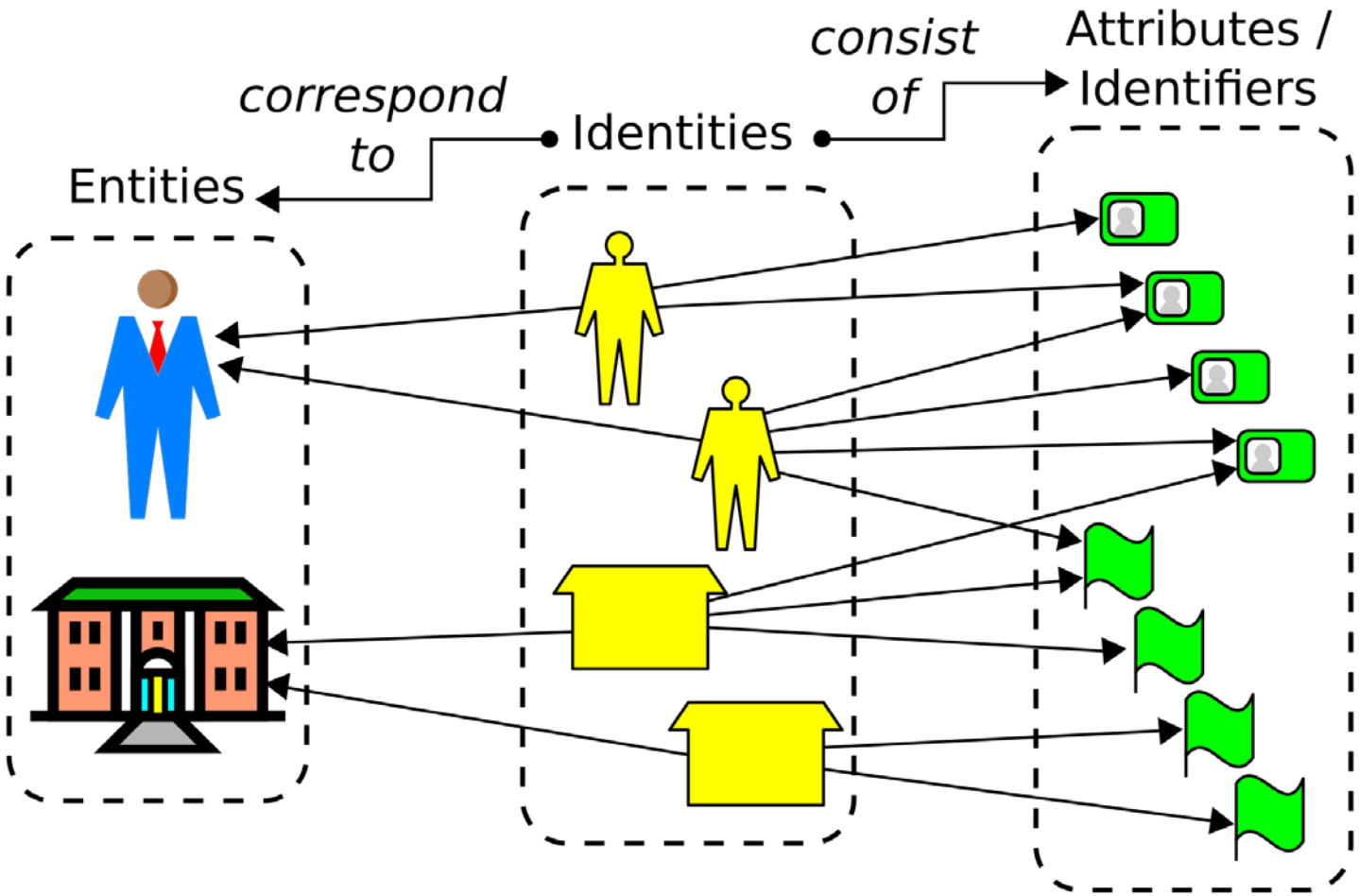



Image source: https://en.wikipedia.org/wiki/Identity_management

Image Source: http://i.imgur.com/r8cY83z.jpg

# What makes up a digital identity?

In other words….what do you already know about your users ?

# *Sources of Identity - Students*

- Student number / identifier
- Name
- Email address
- Qualifications
- Course registration
- Marks, exam results
- Password
- ….

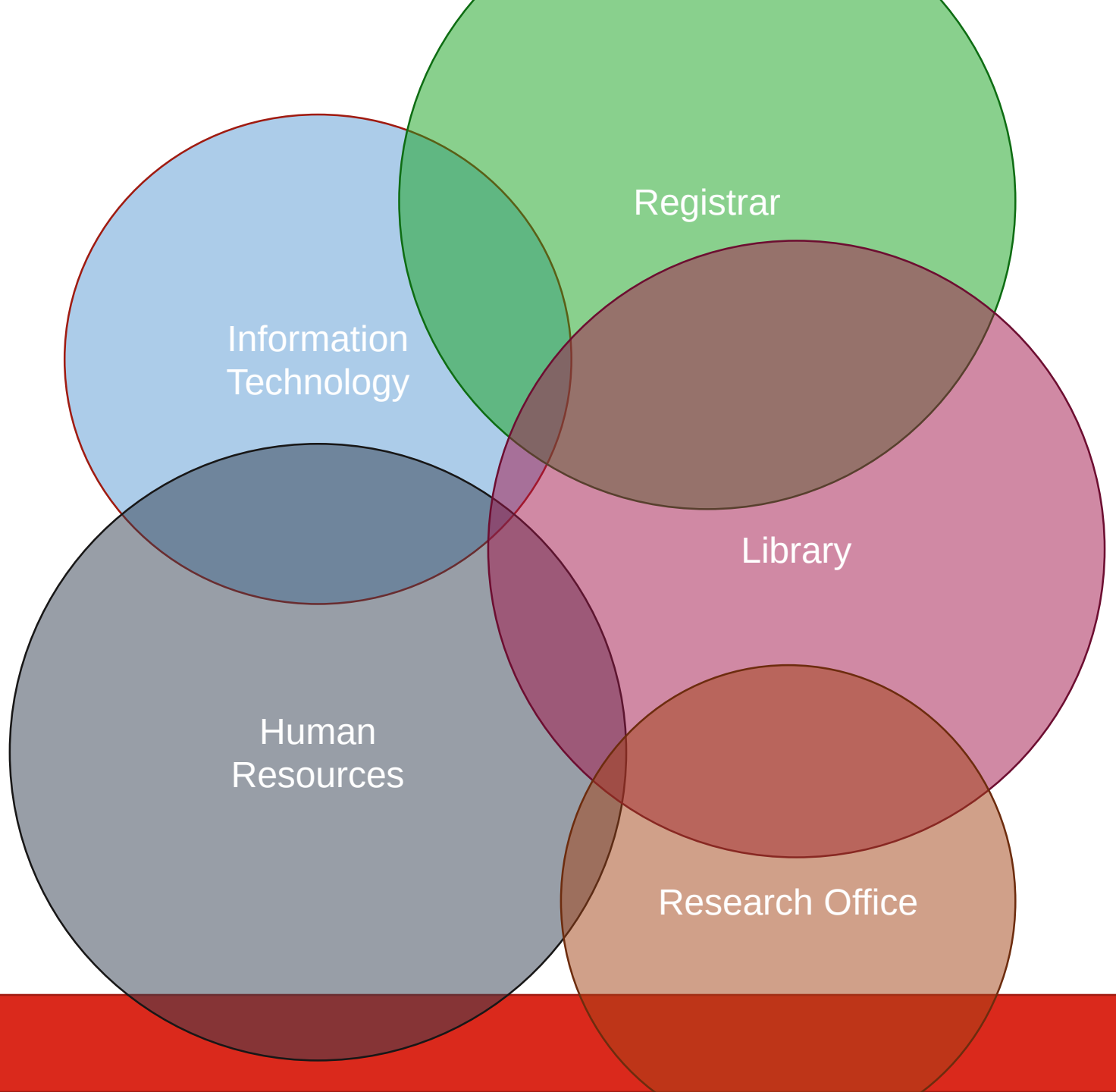
# *Sources of Identity - Staff*

- Employee number /identifier
- Name, address, phone number
- Contract status
- Password
- Email address
- Faculty, department, division
- Committee membership
- …

# *Sources of Identity – Researchers*

- Current research
- Grants
- Publications, research output?
- …

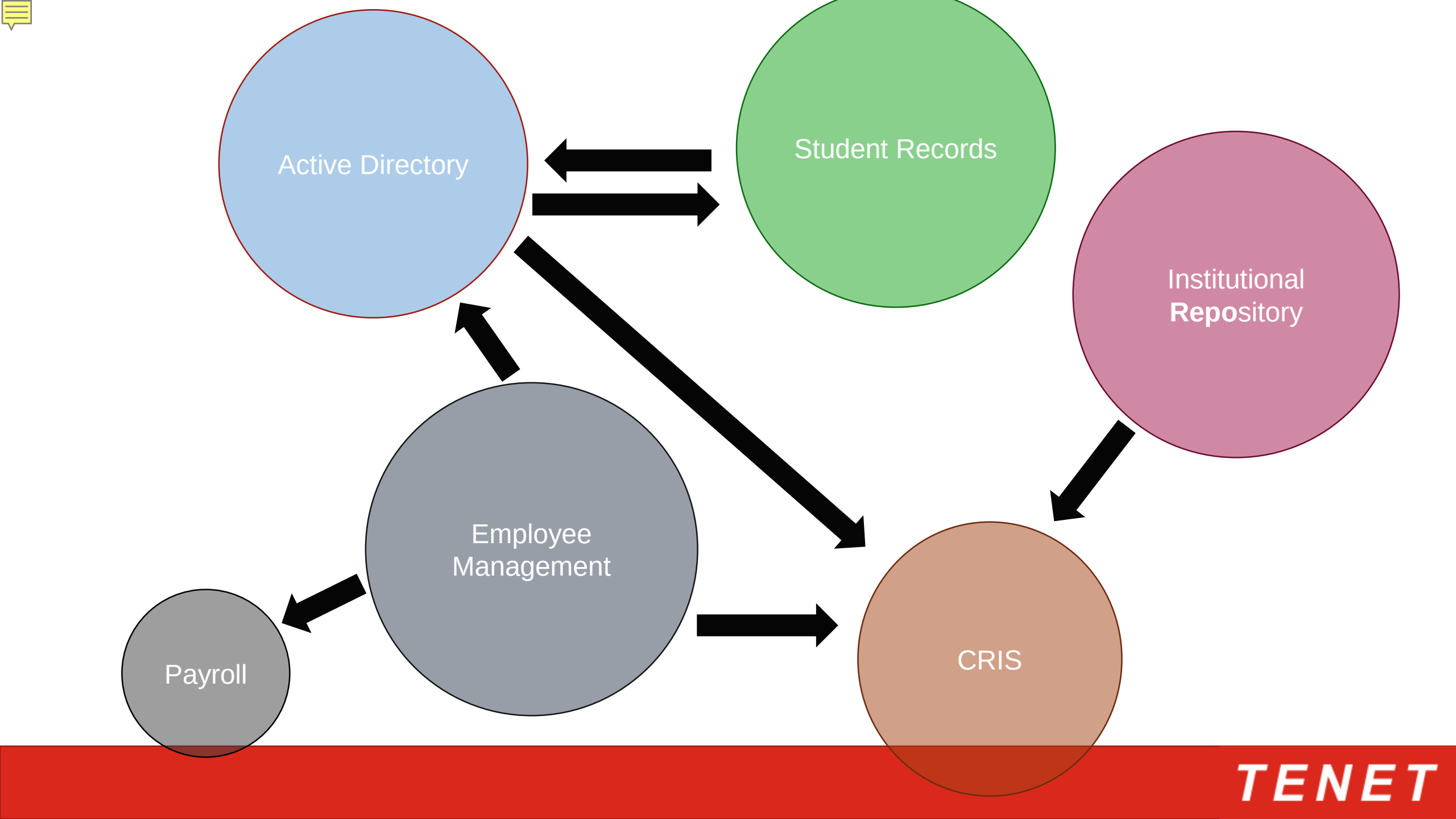
*Where do we get these attributes ?*


Registrar
Information Technology
Library
Human Resources
Research Office

# *Systems that use Identity*

where does identity live in your institution?

- Active Directory
- Student records
- Human resources/employee management
- Payroll
- Current research information system (CRIS)
- Grant management system
- Institutional repositories
- Alumni relations
- …


Active Directory
Student Records
Institutional
Repository
Employee
Management
Payroll
CRIS

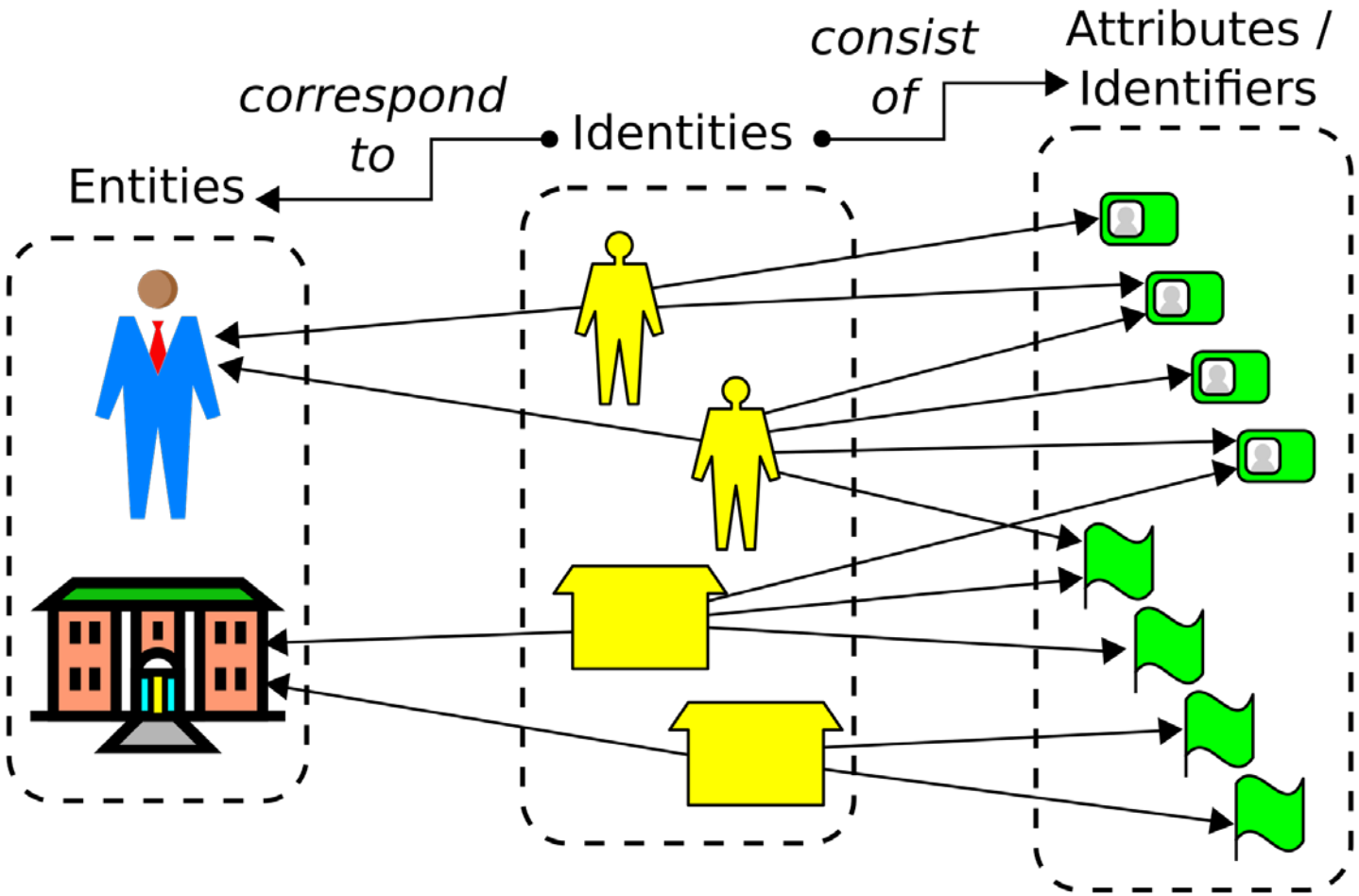



Image source: https://en.wikipedia.org/wiki/Identity_management

# *Person Identifiers*

- Username
- National ID
- Passport number
- Student number
- Employee/staff number
- Email address?
- ORCID iD
- GUID

Privacy Implications ?

When/How do these attributes change?

Can there be duplication ?

Do we agree on formatting ?

*What makes a good identifier?*

- Persistent vs transient
- Transferable / reassignment
- Unique

- Pseudo-anonymous
- Opaque
- Pseudonym
- Targeted

- Should be generated
- Must be opaque and uni-directional
  - e.g. a SHA-256 hash
- Think about making them targeted

Open Researcher and Contributor Identifier

https://orcid.org/0000-0003-2845-6969

Persistent, opaque
Institutionally independent

Like a Digital Object identifier (DOI) for people

# *Identity Management*

“enables the right individuals to access the right resources, at the right time, for the right reasons” (Wikipedia)

# Evolution of Identity Techniques

### Application Centric IdM

- Services activated, but little interaction between them
- Applications have distinct userID/password pairs of their own

### Centralizing Campus Directory & Sign-On

- Services are easier to turn on
- Users are using same password
- Campus SSO users sign in once
- Applications cannot see the user's password

### Federated SSO

- Faster service turn-up time – config and go
- Minimized attack/risk surface inherent in design
- Services outside your domain more easily enabled

# Evolution of Identity Techniques

## Application Centric IdM

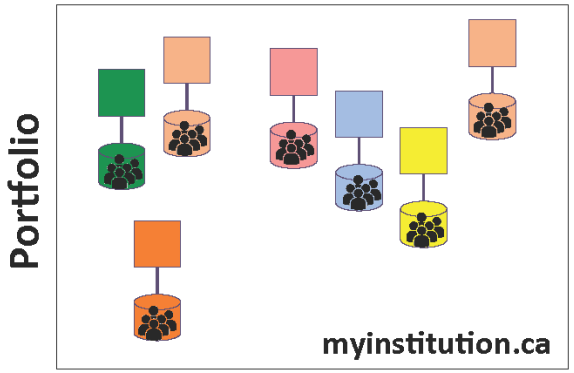
- Services activated, but little interaction between them
- Applications have distinct userID/password pairs of their own

## Centralizing Campus Directory & Sign-On

- Services are easier to turn on
- Users are using same password
- Campus SSO users sign in once
- Applications cannot see the user's password

## Federated SSO

- Faster service turn-up time – config and go
- Minimized attack/risk surface inherent in design
- Services outside your domain more easily enabled



# Evolution of Identity Techniques

### Application Centric IdM

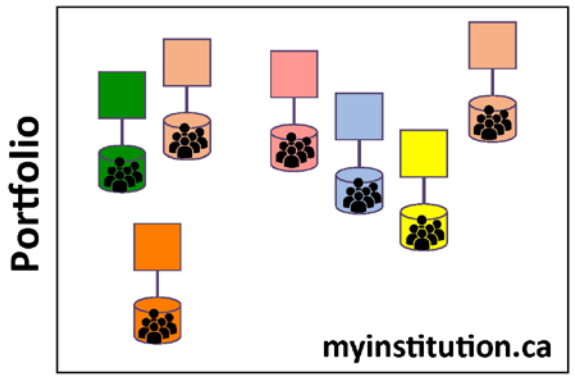
- Services activated, but little interaction between them
- Applications have distinct userID/password pairs of their own

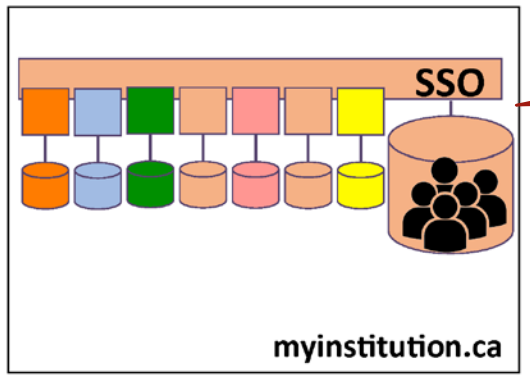
### Centralizing Campus Directory & Sign-On

- Services are easier to turn on
- Users are using same password
- Campus SSO users sign in once
- Applications cannot see the user's password

### Federated SSO

- Faster service turn-up time – config and go
- Minimized attack/risk surface inherent in design
- Services outside your domain more easily enabled




What do we need to get here ?

Image Source: https://imgflip.com

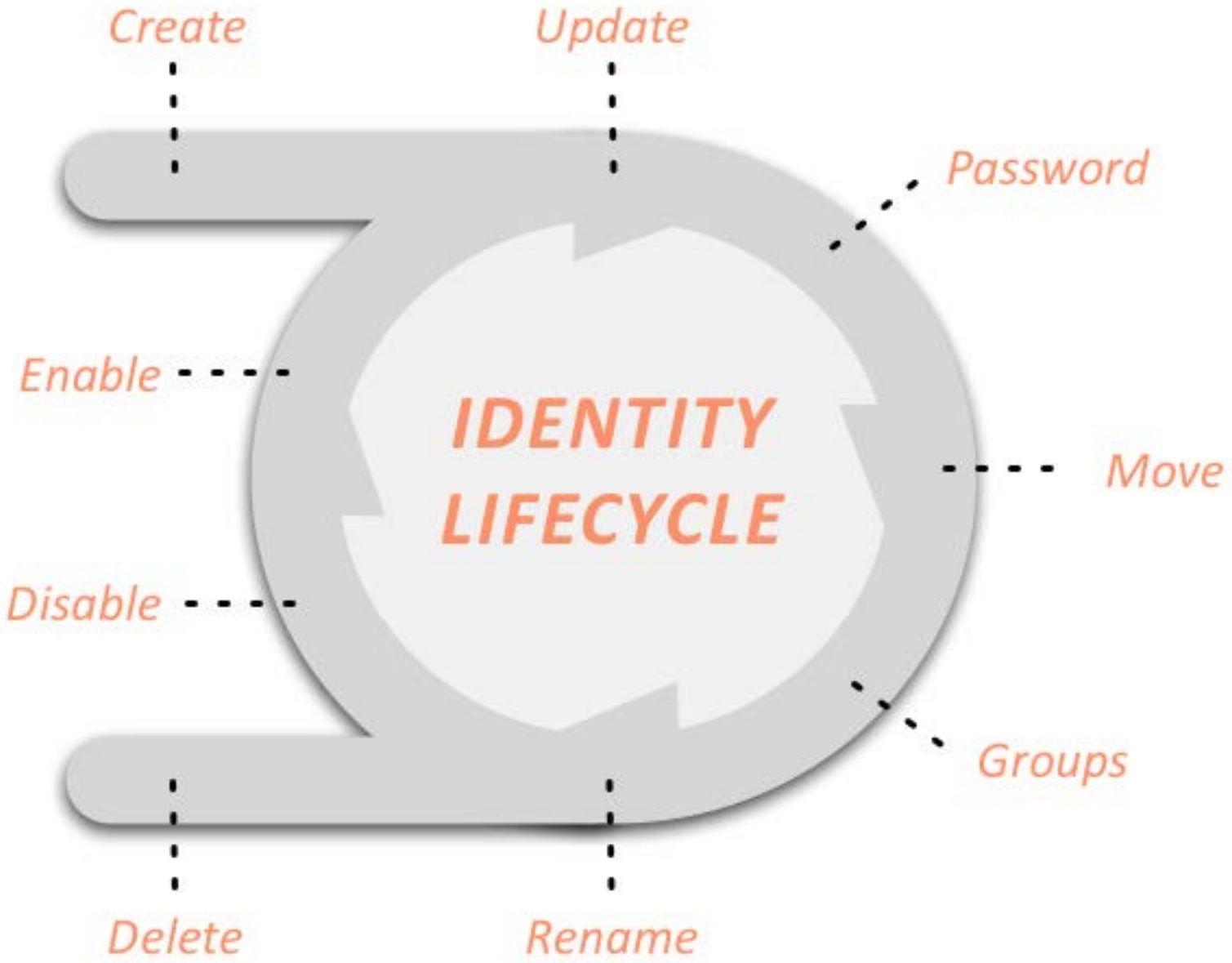



Image Source:http://cwsolutions.ca/cws2/wp-content/uploads/2014/02/RH5DQJK.png

- If you haven’t already done so, conduct an institution-wide audit of identity to determine who has what attributes
- Determine the authority for each attribute, e.g:
  - Email address -> IT department
  - Student numbers -> Registrar
  - Student name -> Registrar
  - Staff name -> Human resources
- Determine consumers for each attribute
- Determine what constraints exist for each attribute:
  - Name field is 100 chars at authority, but CRIS system only accepts 80 chars

- You probably already have some processes to share information between departments, but:
  - Make sure these are aligned with the audit results (right authority)
  - Use common language and descriptions (what do we mean by givenName?)
  - Start aligning the constraints (if smallest name field is 80 chars and this cannot be changed, use 80 char names)
  - Introduce update processes to ensure identities remain in sync (all consumers are told when a change happens at the authority)

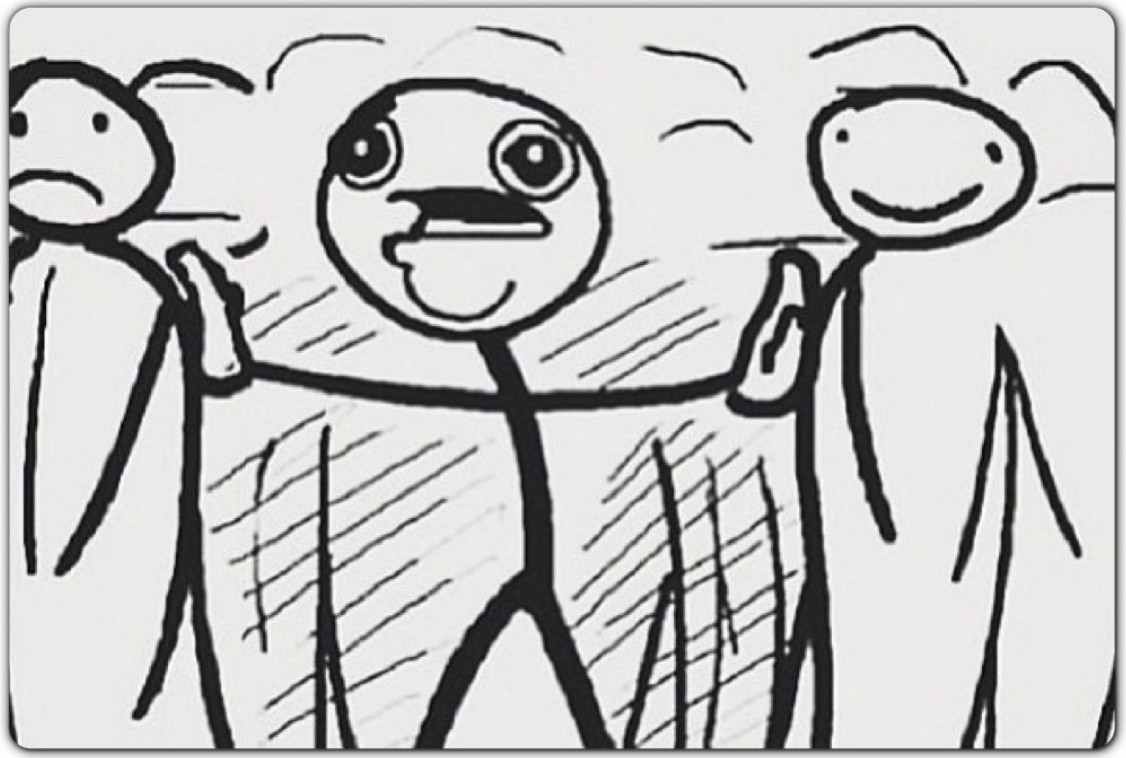
- You need institutional buy-in – can be hard to get
- Take small steps, easy wins
  - but do not lose sight of the big picture
- These interim steps do **not** need to depend on technology

# *Home Work ?!*

Do some reading on Kim Cameron’s 7 laws of identity

It may be old, but it is still very valid!

DID SOMEONE SAY



FOOD?!

memecrunch.com