TENET
Tertiary Education and Research Network of South Africa

Identity

An introduction

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

What is an identity?

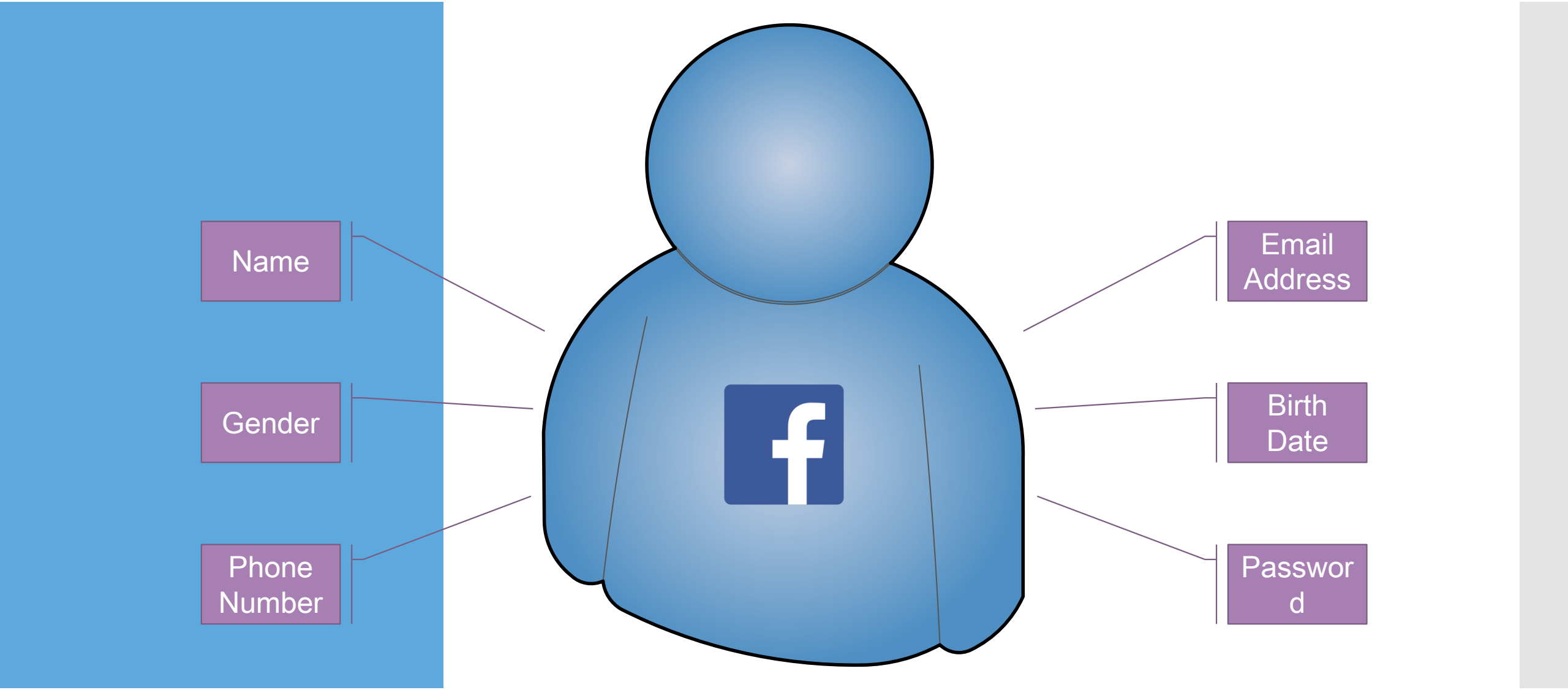
A set of attributes related to an entity (ISO/IEC 24760-1)

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

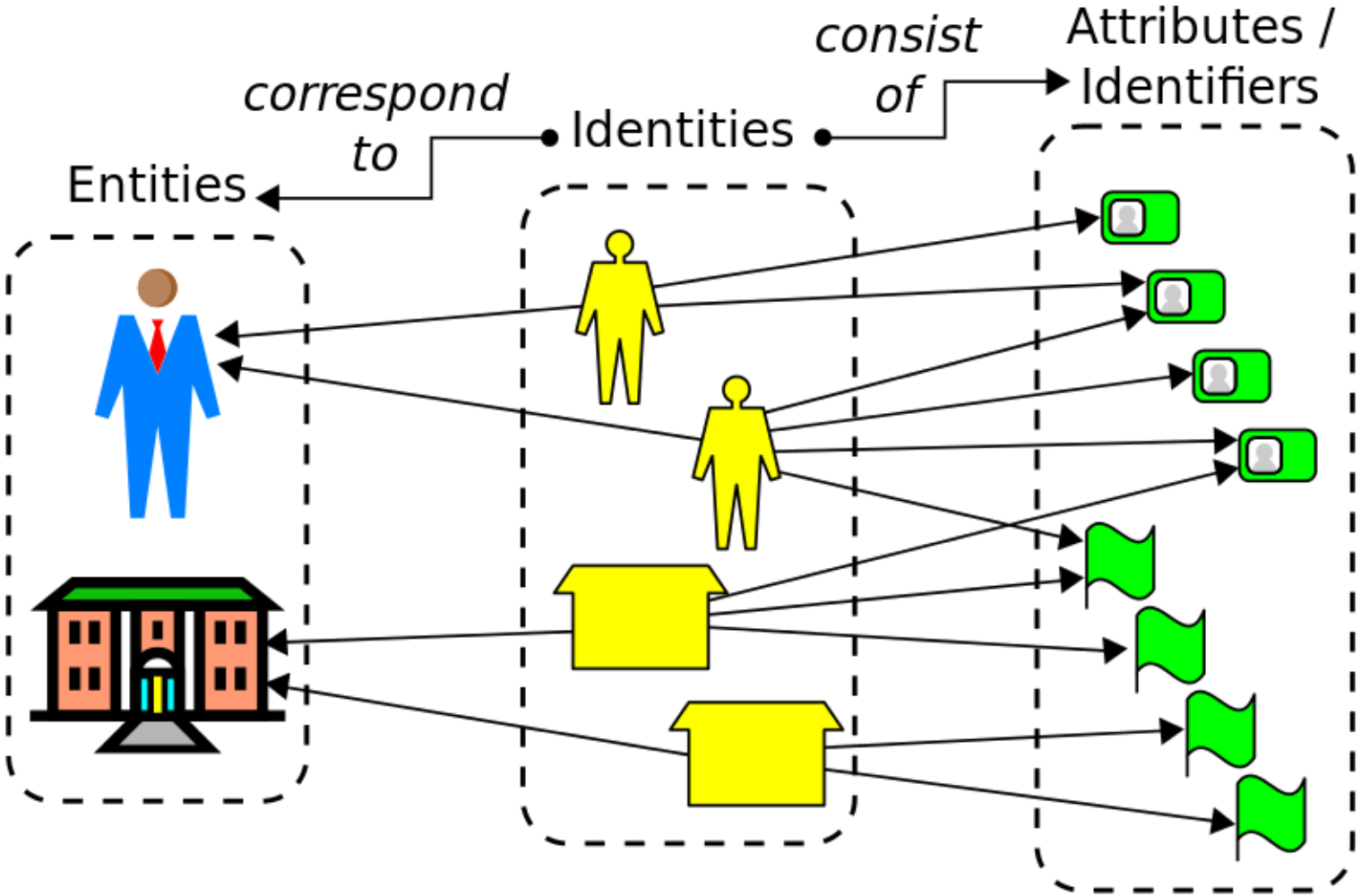
entity (n): a thing with distinct and independent existence.

We have lots of different types of entities in the identity space…

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION



SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION



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

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

What makes up your digital identity?

aka what do you already know about your users?

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

Sources of identity - students

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

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

Sources of identity - staff

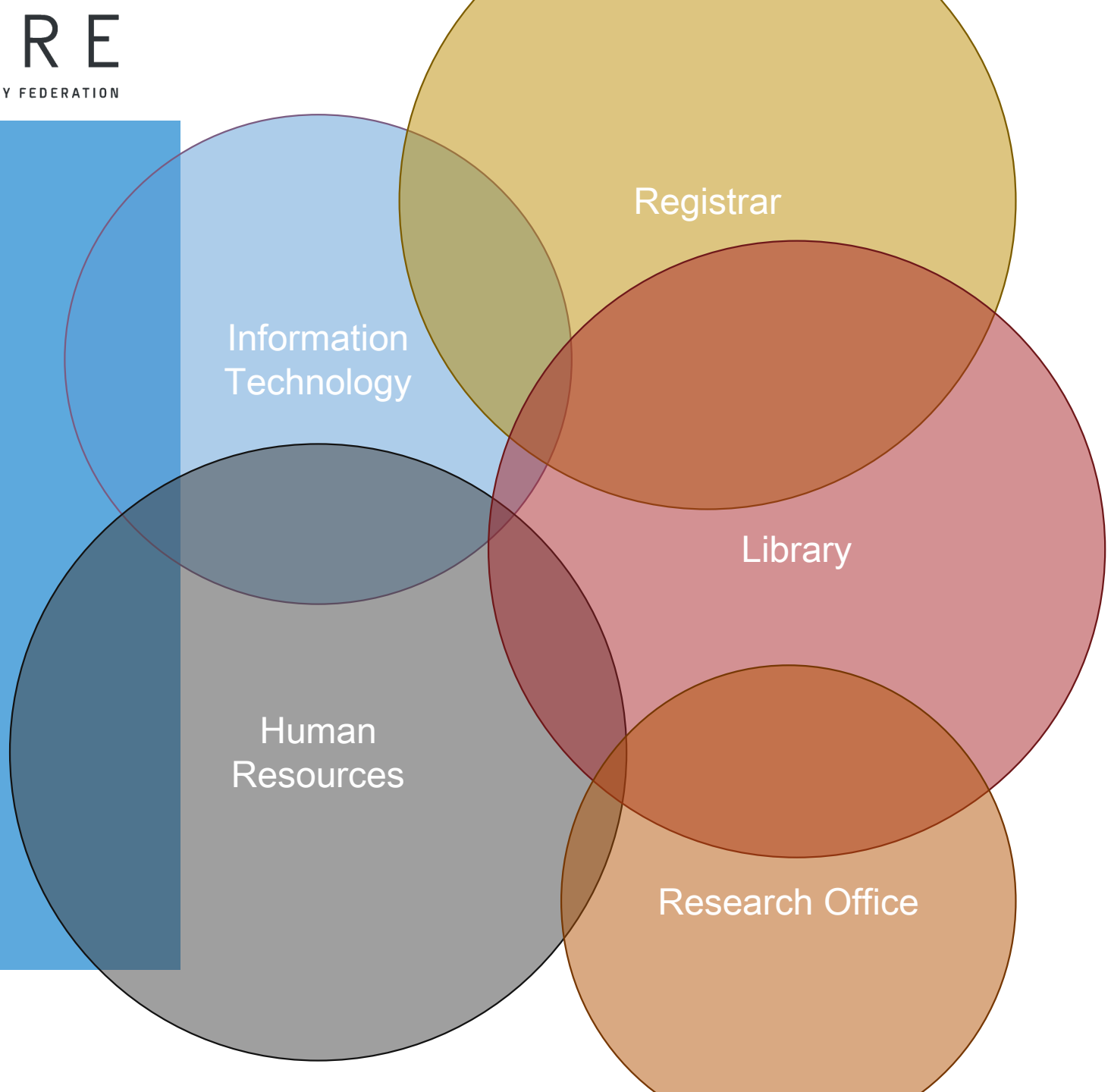
- Employee number / identifier
- Name, address, phone number
- Contract status
- Password
- Email address
- Faculty, department, division
- Committee membership
- …

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

Sources of identity – academic & research

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

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION



SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

Systems using identity

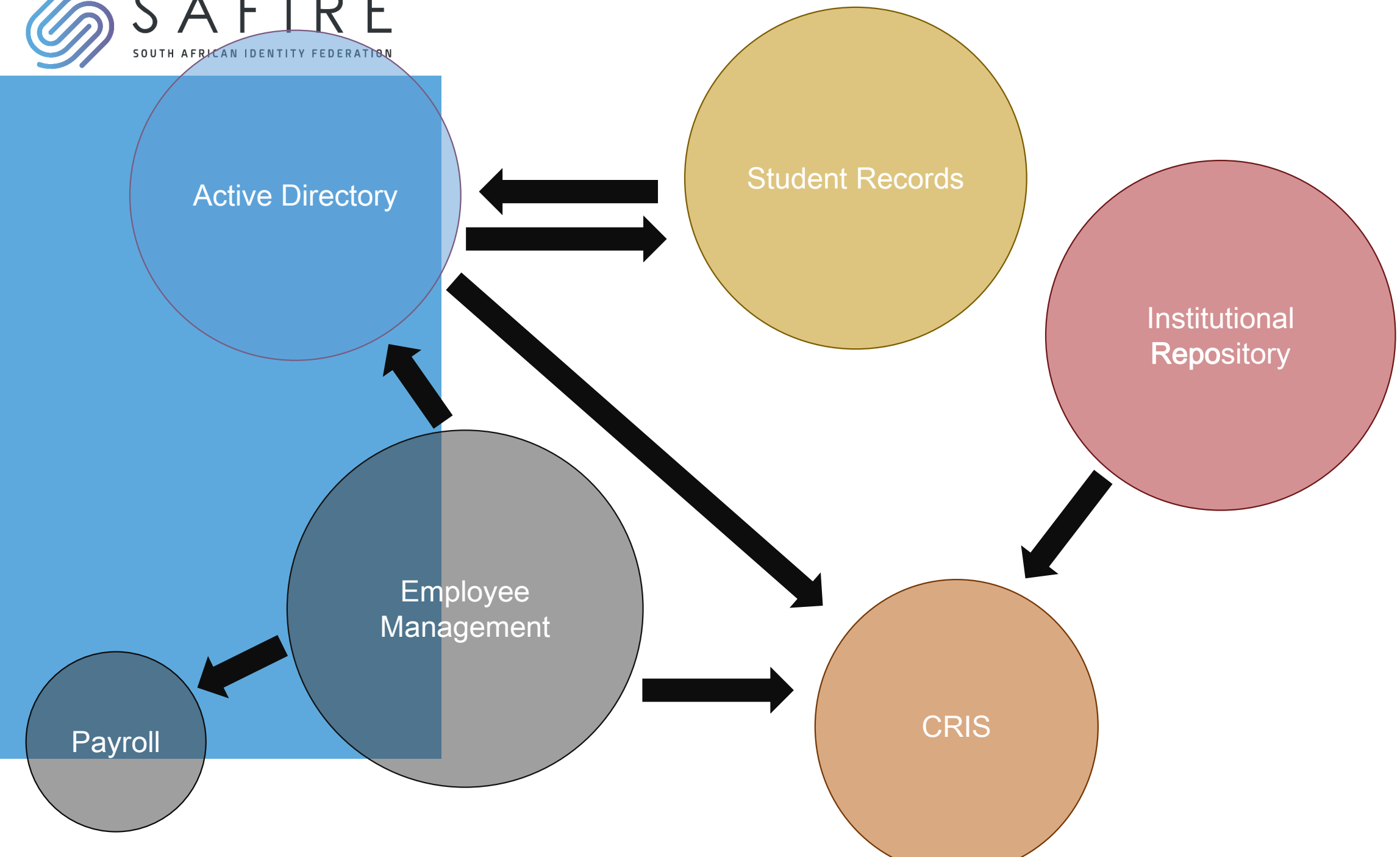
Where does identity live in your institution?

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

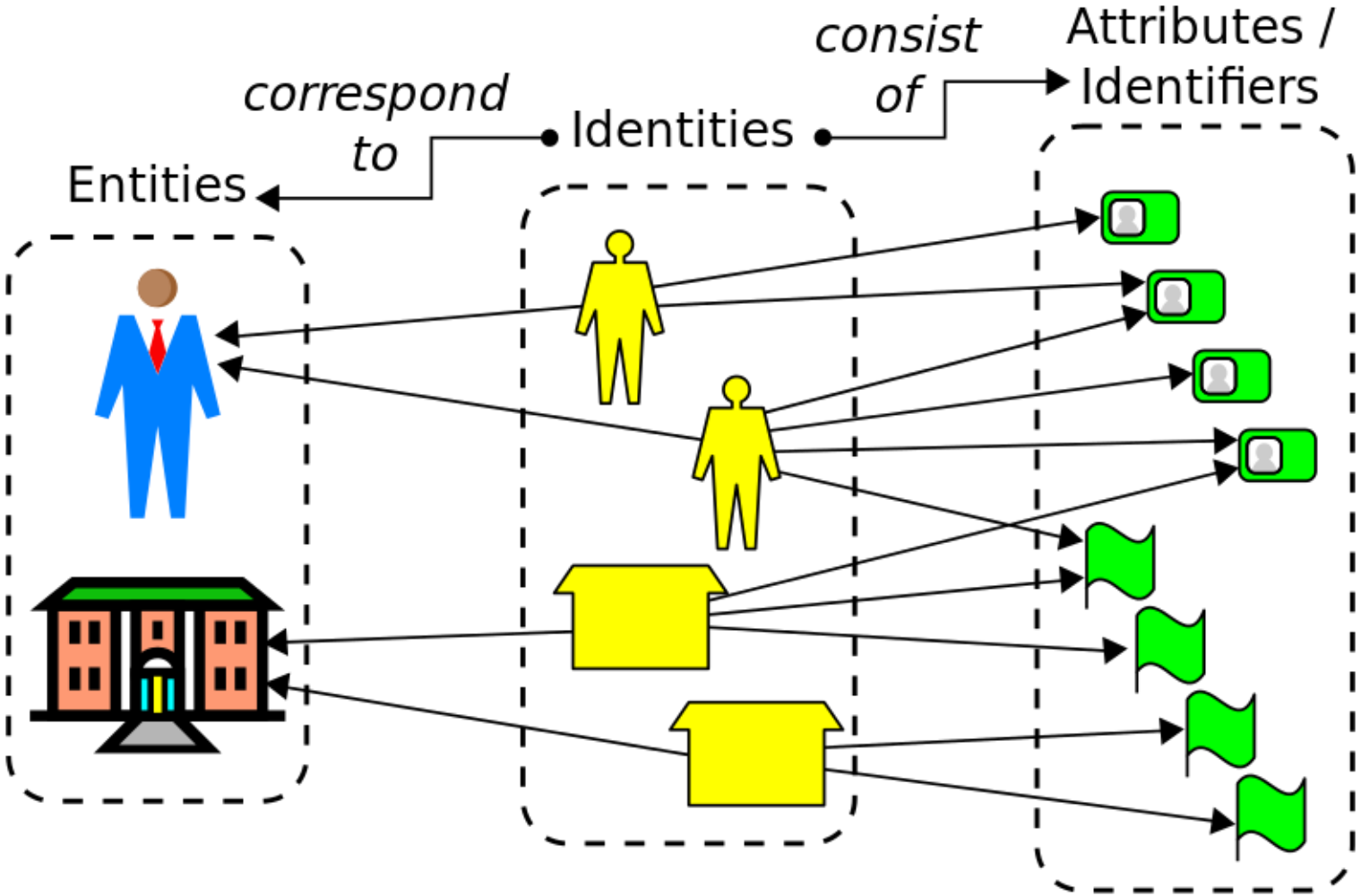
Systems using identity

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

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION



SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION



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

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

Person Identifiers

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

Person Identifiers

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

What are the privacy implications

Do we agree on formatting?

In what circumstances can they change?

Is there ever duplication?

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

What makes a good person identifier?

4NF

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

Identifier concepts/terminology

- Persistent vs transient
- Transferable / reassignment
- Unique

- Pseudo-anonymous
- Opaque
- Pseudonym
- Targeted

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

Privacy-preserving identifiers

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

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

ORCID iD

- Open Researcher and Contributor Ide
- https://orcid.org/0000-0002-1825-0097
- Persistent, opaque
- Institutionally independent
- Like a DOI for people

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

Identity Management

"enables the right individuals to access the right resources at the right times and 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

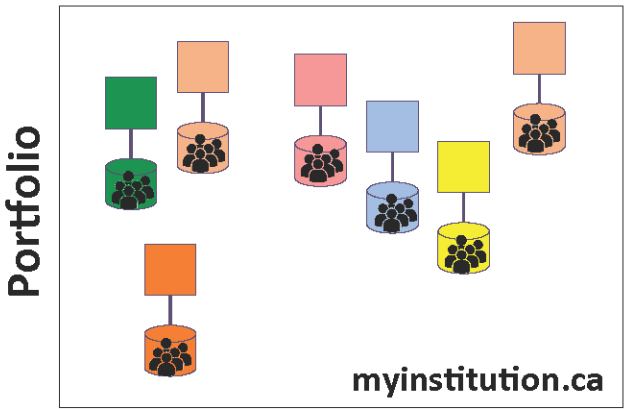
- Services activated, but little interaction between them
- Applications have distinct userID/password pairs of their own

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

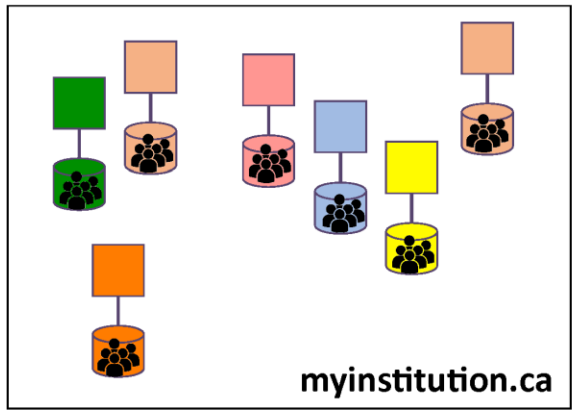
Centralizing Campus Directory & Sign-On

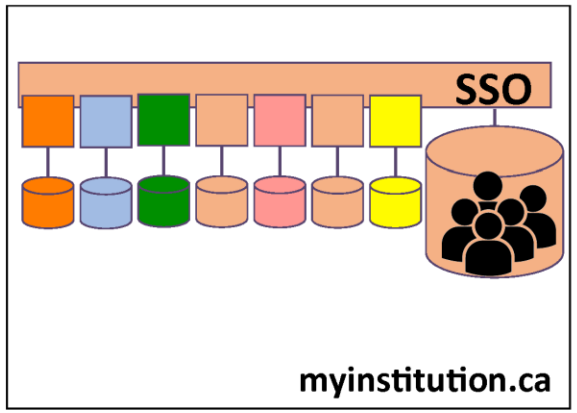
- Services are easier to turn on
- Users are using same password
- Campus SSO users sign in once
- Applications cannot see the user's password

Federated SSO

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

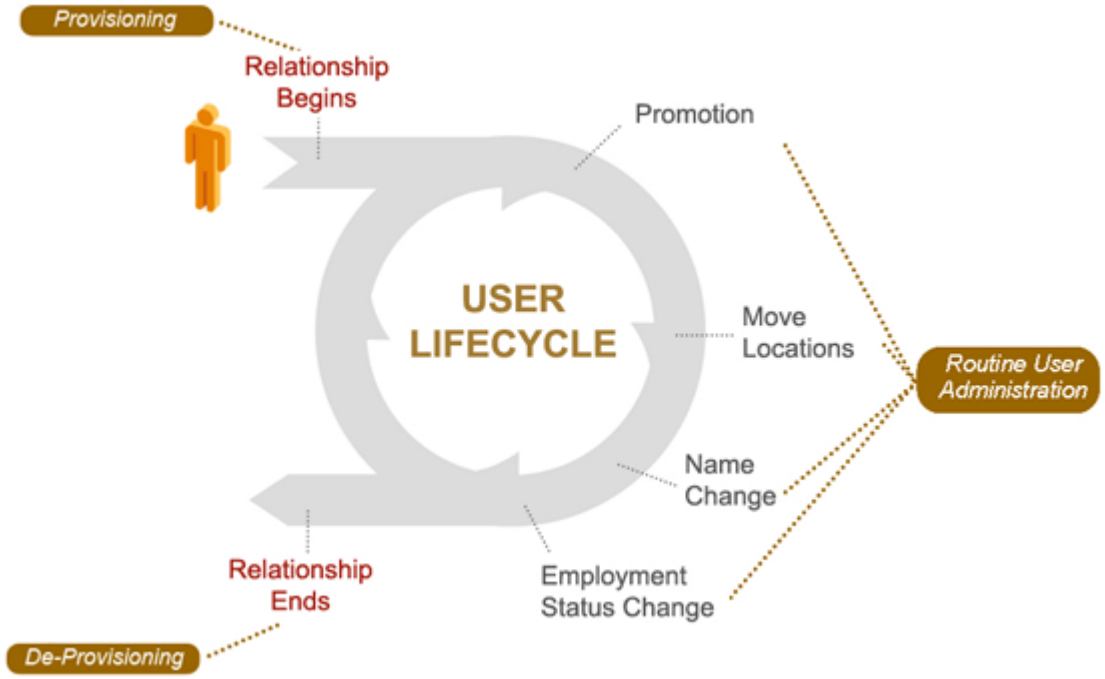
What is needed to get to this stage?





SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

Identity Management Life Cycle



http://www.ithancreek.com/identity_management.asp

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

Centralising identity – authoritative sources

- 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

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

Centralising identity – interim steps (1)

- 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)

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

Centralising identity – interim steps (2)

- 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

SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION

What are the small steps?