IAM
Just-In-Time Provisioning

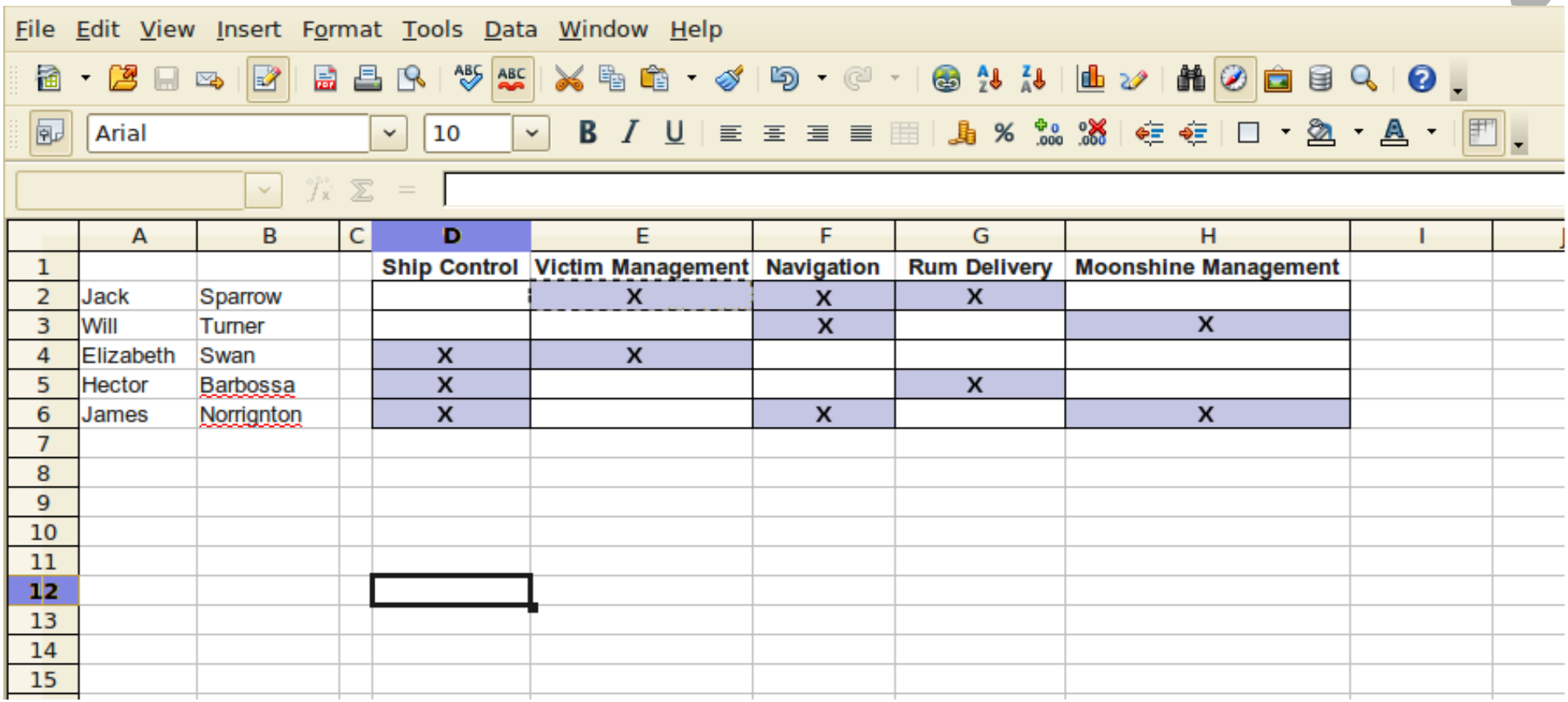
Katarína Valaliková
k.valalikova@evolveum.com

Agenda

- Story of one company
- What is Identity & Access Management?
- More about Identity Management
- Federation
- Demo

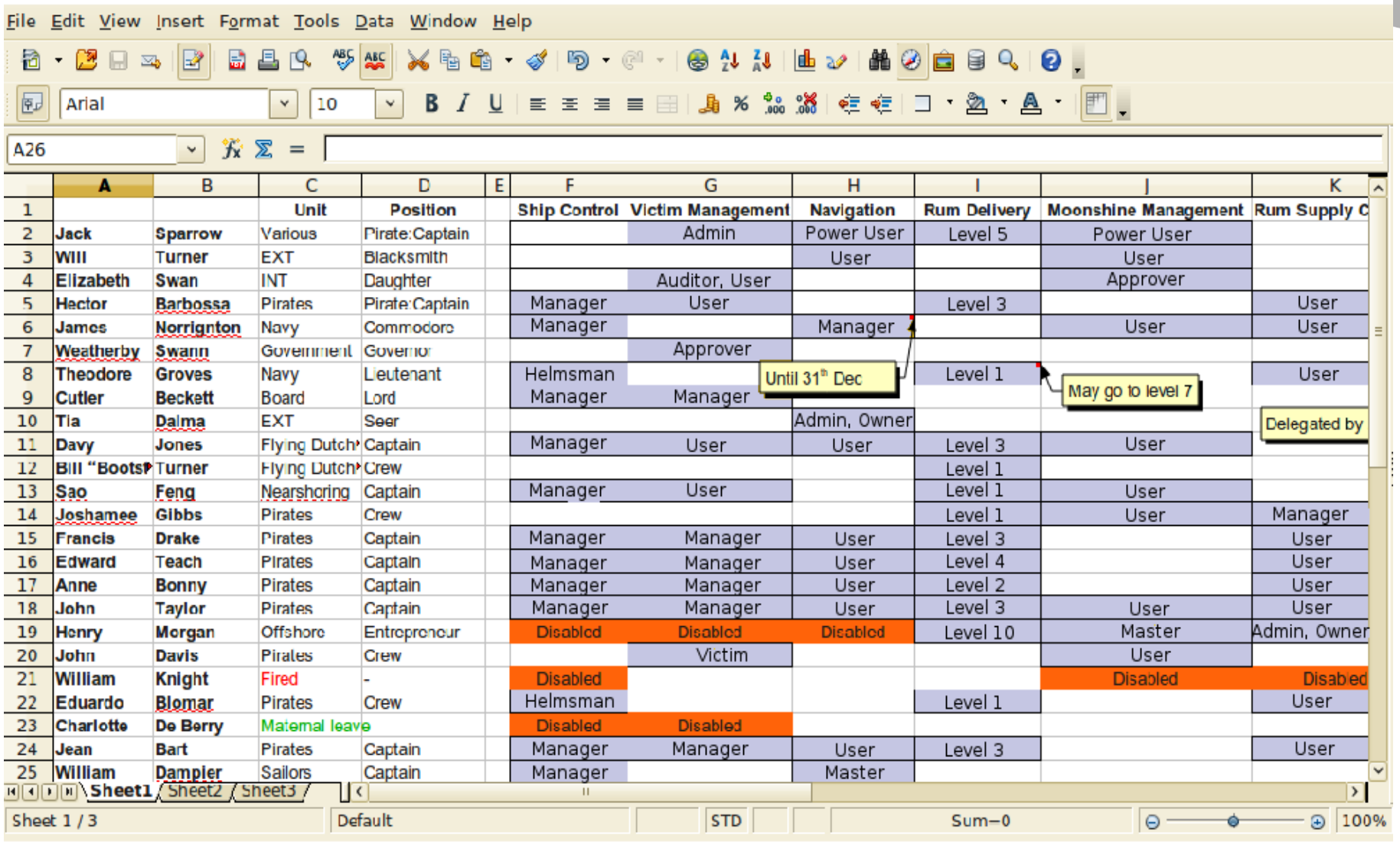
Story of One Company

Simple Easy Start



	A	B	C	D	E	F	G	H	I
1				Ship Control	Victim Management	Navigation	Rum Delivery	Moonshine Management	
2	Jack	Sparrow			X	X	X		
3	Will	Turner				X		X	
4	Elizabeth	Swan		X	X				
5	Hector	Barbossa		X			X		
6	James	Norrignton		X		X		X	
7									
8									
9									
10									
11									
12									
13									
14									
15									

… but the Company's growing up…



File Edit View Insert Format Tools Data Window Help

Arial 10

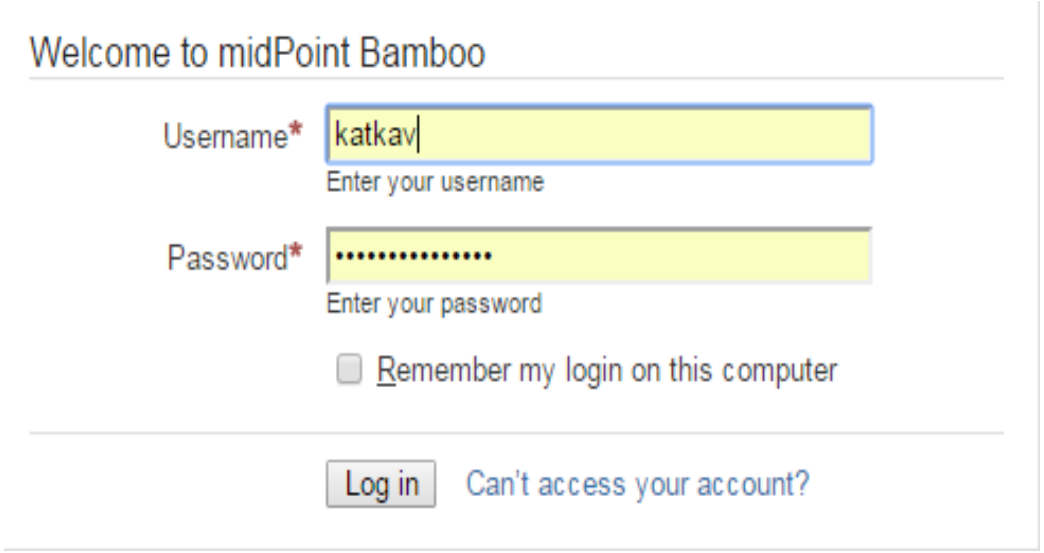
A26

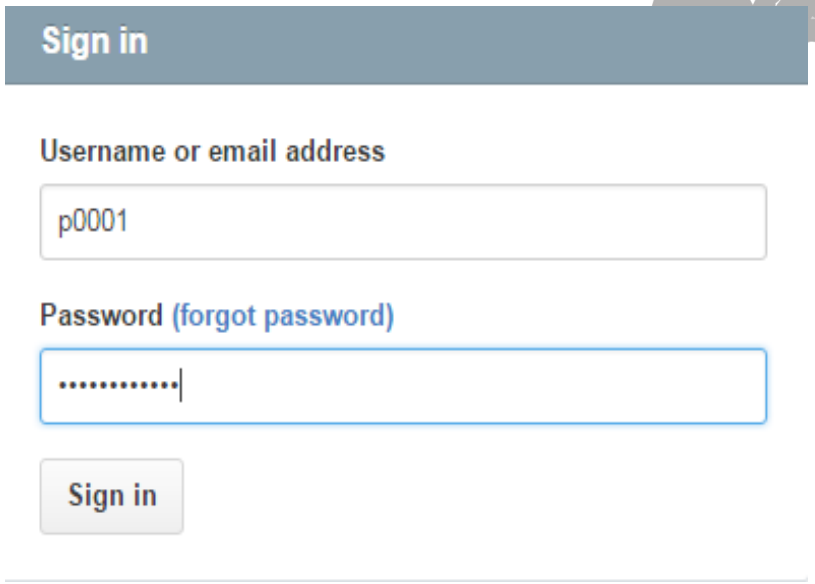
	A	B	C	D	E	F	G	H	I	J	K
1			Unit	Position		Ship Control	Victim Management	Navigation	Rum Delivery	Moonshine Management	Rum Supply C
2	Jack	Sparrow	Various	Pirate:Captain			Admin	Power User	Level 5	Power User	
3	Will	Turner	EXT	Blacksmith				User		User	
4	Elizabeth	Swan	INT	Daughter			Auditor, User			Approver	
5	Hector	Barbossa	Pirates	Pirate:Captain		Manager	User		Level 3		User
6	James	Norrington	Navy	Commodore		Manager		Manager		User	User
7	Weatherby	Swann	Government	Governor			Approver				
8	Theodore	Groves	Navy	Lieutenant		Helmsman		Until 31th Dec	Level 1		User
9	Cutler	Beckett	Board	Lord		Manager	Manager			May go to level 7	
10	Tia	Dalma	EXT	Seer				Admin, Owner			Delegated by
11	Davy	Jones	Flying Dutch	Captain		Manager	User	User	Level 3	User	
12	Bill "Boots"	Turner	Flying Dutch	Crew					Level 1		
13	Sao	Feng	Nearshoring	Captain		Manager	User		Level 1	User	
14	Joshamee	Gibbs	Pirates	Crew					Level 1	User	Manager
15	Francis	Drake	Pirates	Captain		Manager	Manager	User	Level 3		User
16	Edward	Teach	Pirates	Captain		Manager	Manager	User	Level 4		User
17	Anne	Bonny	Pirates	Captain		Manager	Manager	User	Level 2		User
18	John	Taylor	Pirates	Captain		Manager	Manager	User	Level 3	User	User
19	Henry	Morgan	Offshore	Entrepreneur		Disabled	Disabled	Disabled	Level 10	Master	Admin, Owner
20	John	Davis	Pirates	Crew			Victim			User	
21	William	Knight	Fired	-		Disabled				Disabled	Disabled
22	Eduardo	Blomar	Pirates	Crew		Helmsman			Level 1		User
23	Charlotte	De Berry	Maternal leave			Disabled	Disabled				
24	Jean	Bart	Pirates	Captain		Manager	Manager	User	Level 3		User
25	William	Dampier	Sailors	Captain		Manager		Master			

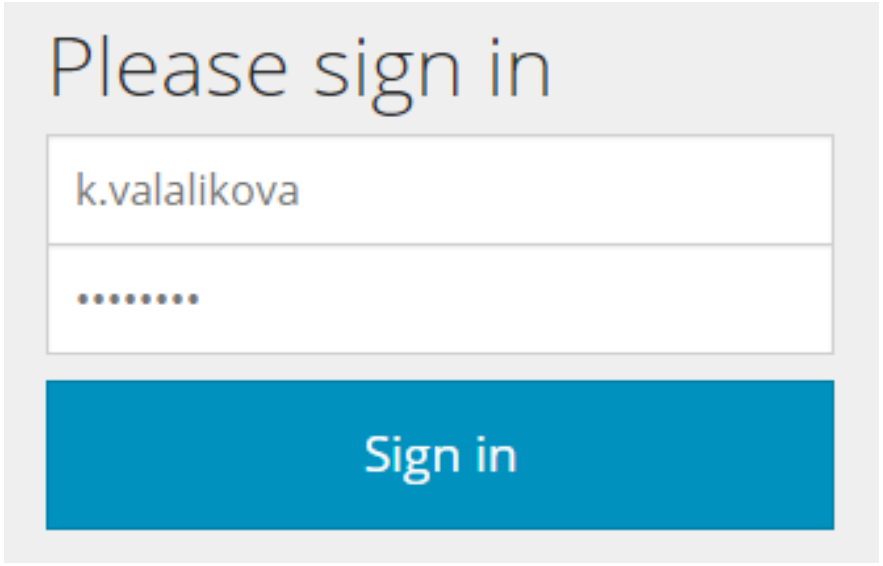
Sheet1 Sheet2 Sheet3

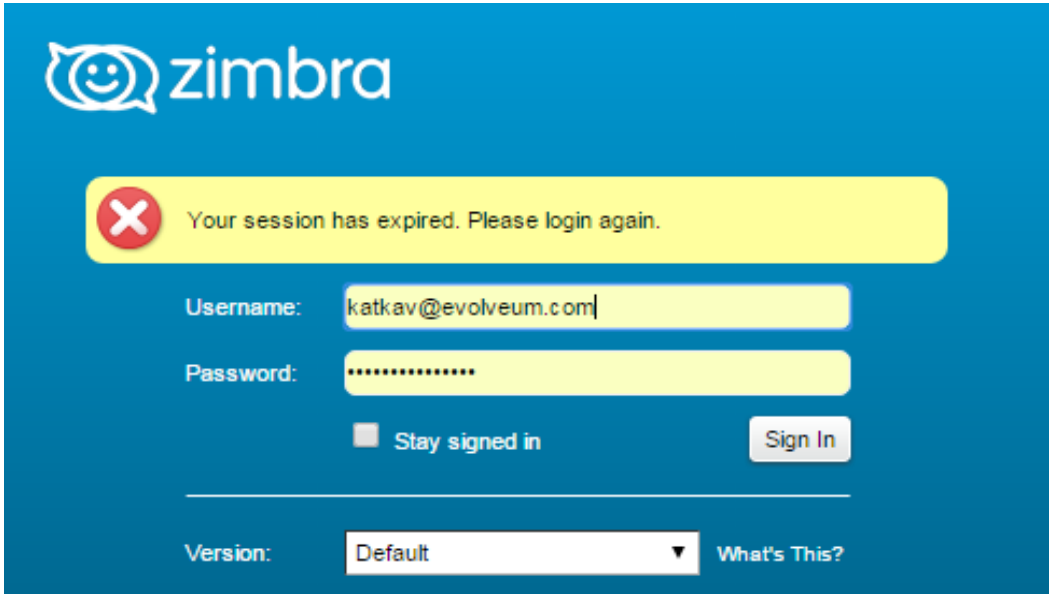
Sheet 1 / 3 Default STD Sum=0 100%

Login Nightmares









Login Nightmares

What's next?

… think about what you need

Basic requirements:

- Which systems can user Norris access?
- What is this 'u0001' account? Who created it? Who's is this 'u0001' account?
- Why this new employee still doesn't have his accounts created?
- Which privileges do I need for this system?
- Where can I reset my password?
- Who can enable my account as fast as possible?
- Who can restrict access for Norris?

… was that sufficient?

Advanced requirements:

- How to eliminate access rights to the minimum for employees?
- How to provide access right for different users?
- How to provide approvals for some access rights?
- How to remove “illegal” access rights?
- How to do approvals cenatralized?
- How to delegate part of the administration to the users?
- How to eliminate the time spending for user administration?

More about Identity and Aceess Management

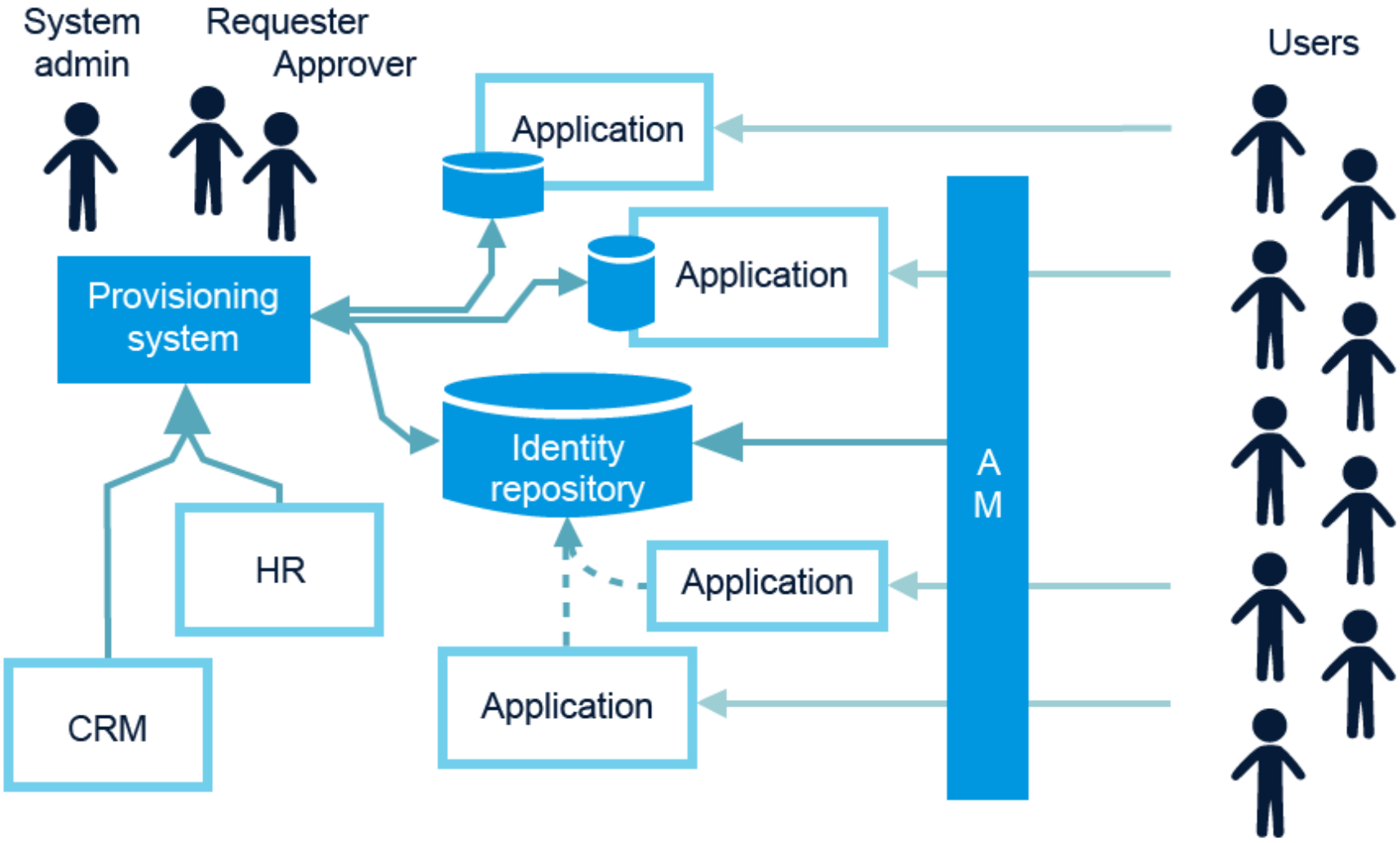
What is NOT Identity Management

It is NOT only Single Sign-On

What is IAM?
Short Answer

Identity management is everything that deals with managing identities in the cyberspace

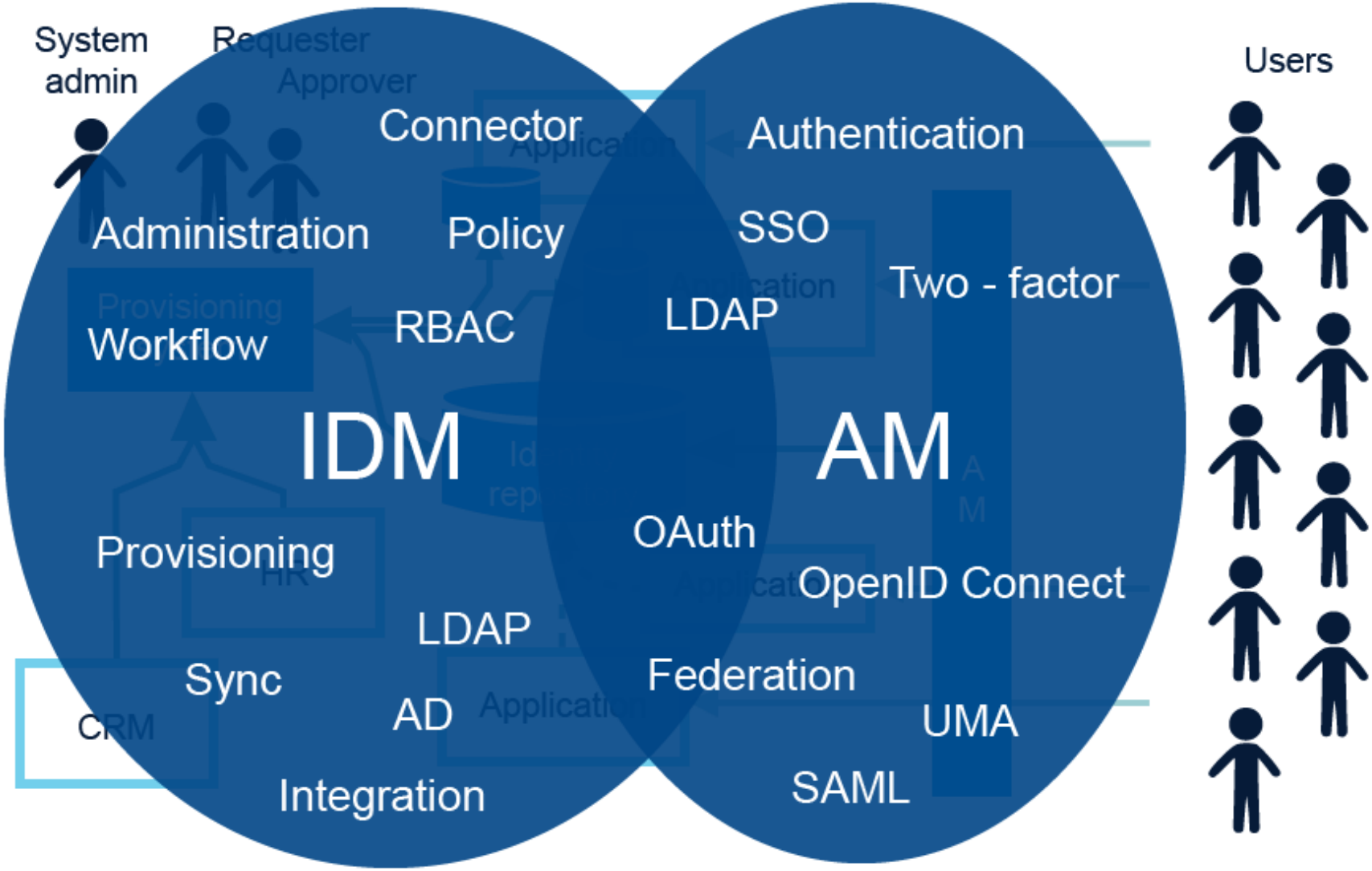
Identity & Access Management



Identity & Access Management Technologies

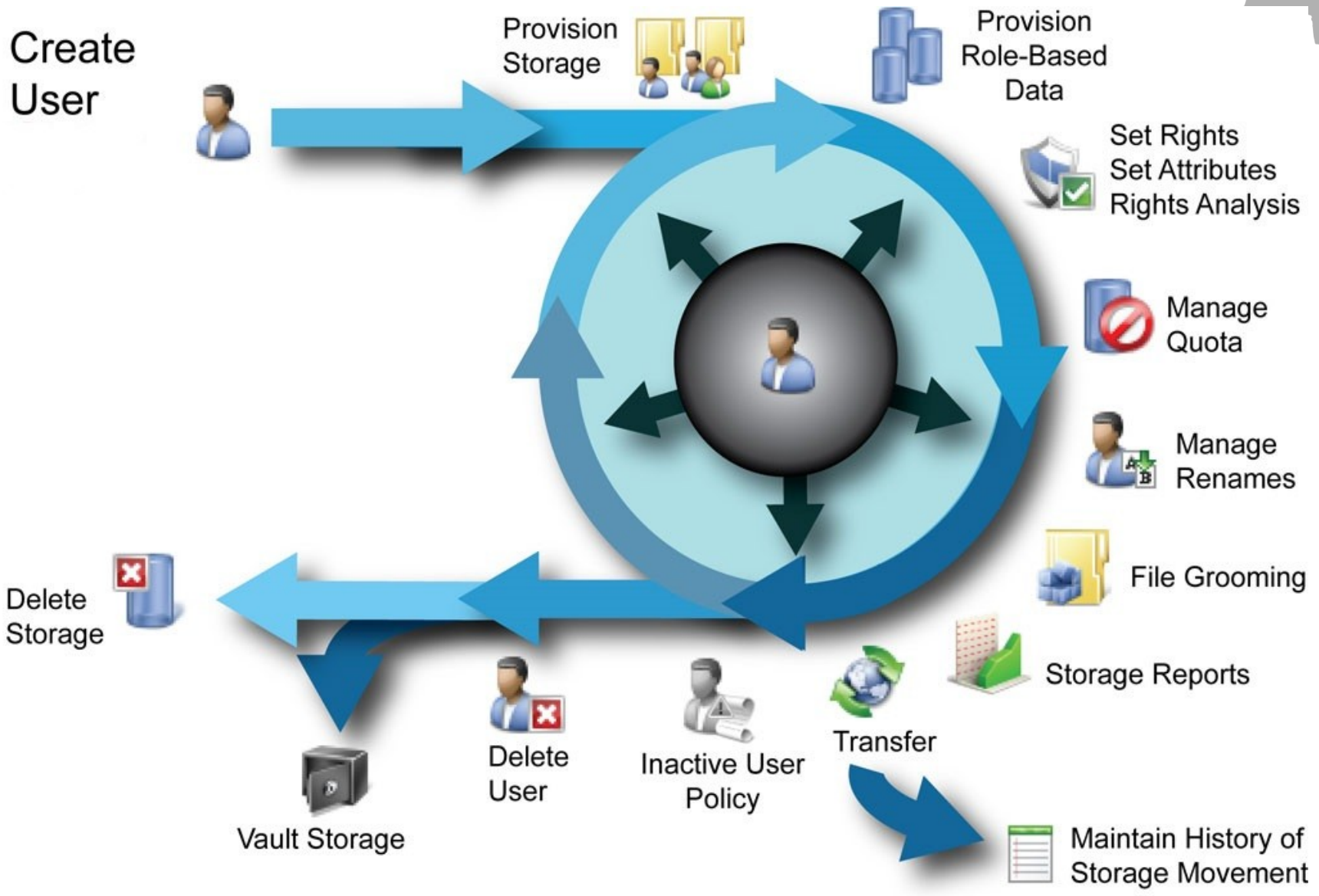
- Identity Repository (IdP) – unified repository containing information about users
- Provisioning System (IdM) – synchronize account data among different systems
- Access Management (SSO) – provide authentication and (partialy) authorization

Identity & Access Management

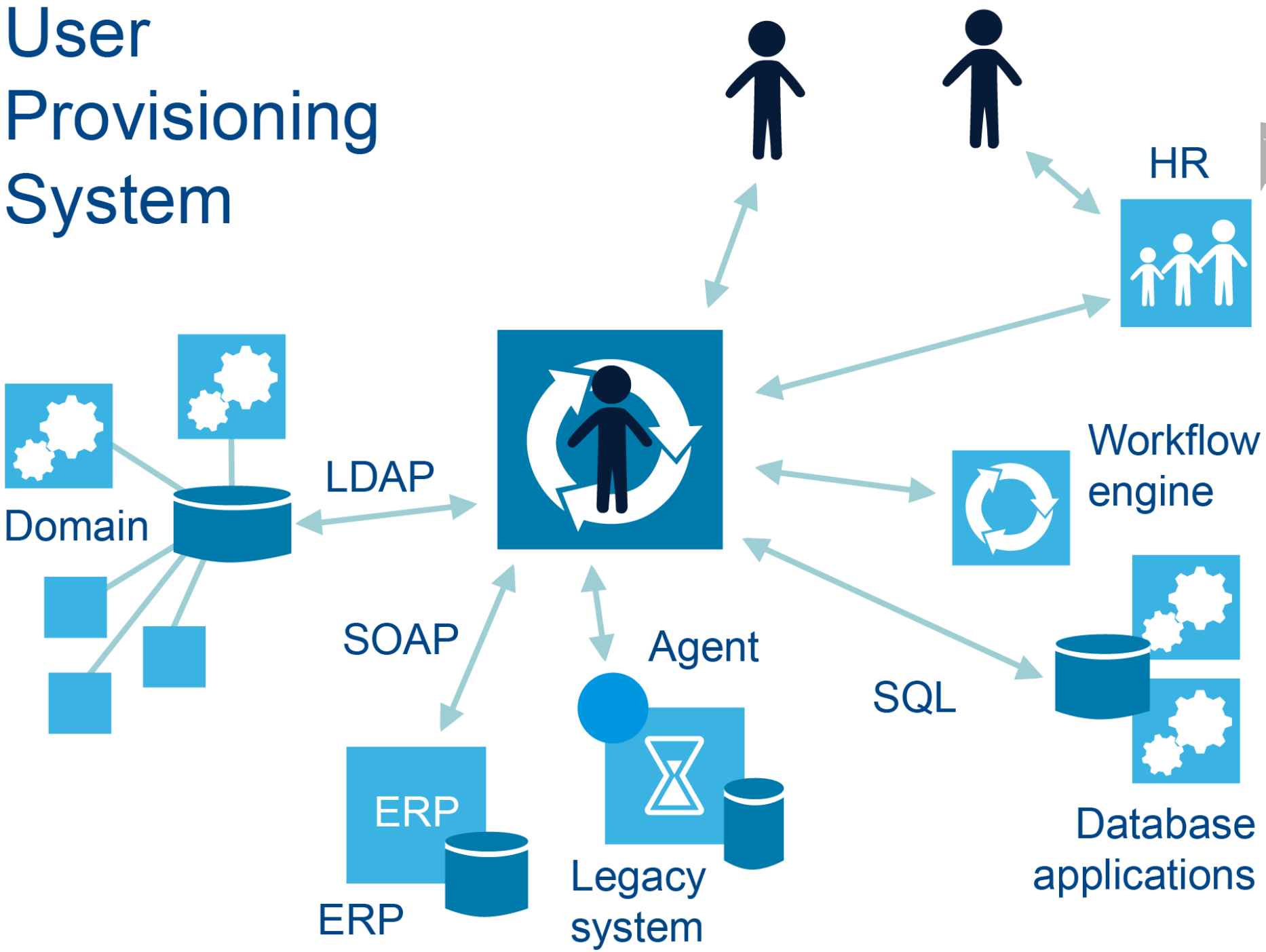


Identity Management Provisioning System

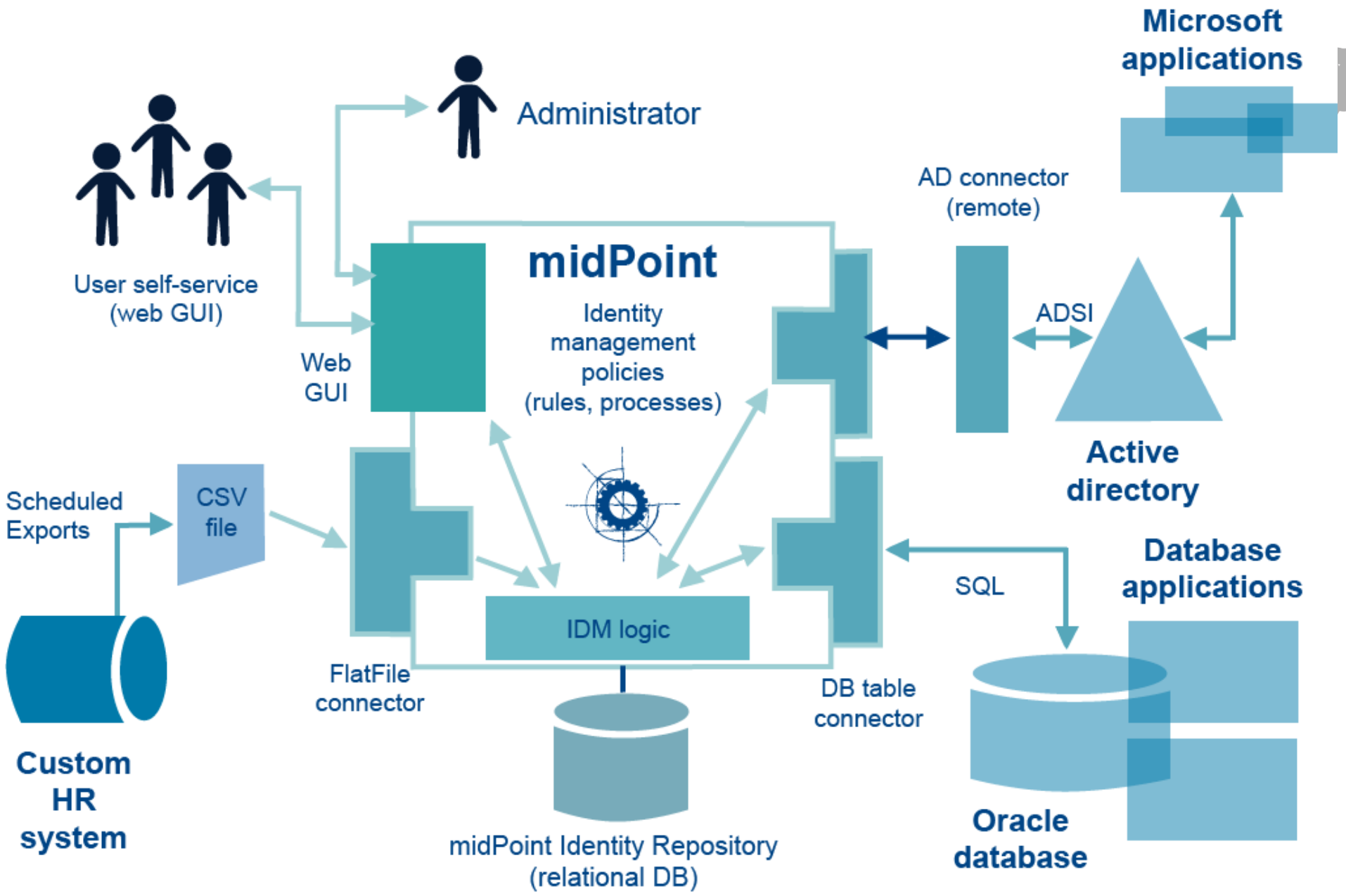
Identity Lifecycle



User Provisioning System



Example midPoint deployment architecture



Access Management

Access Management

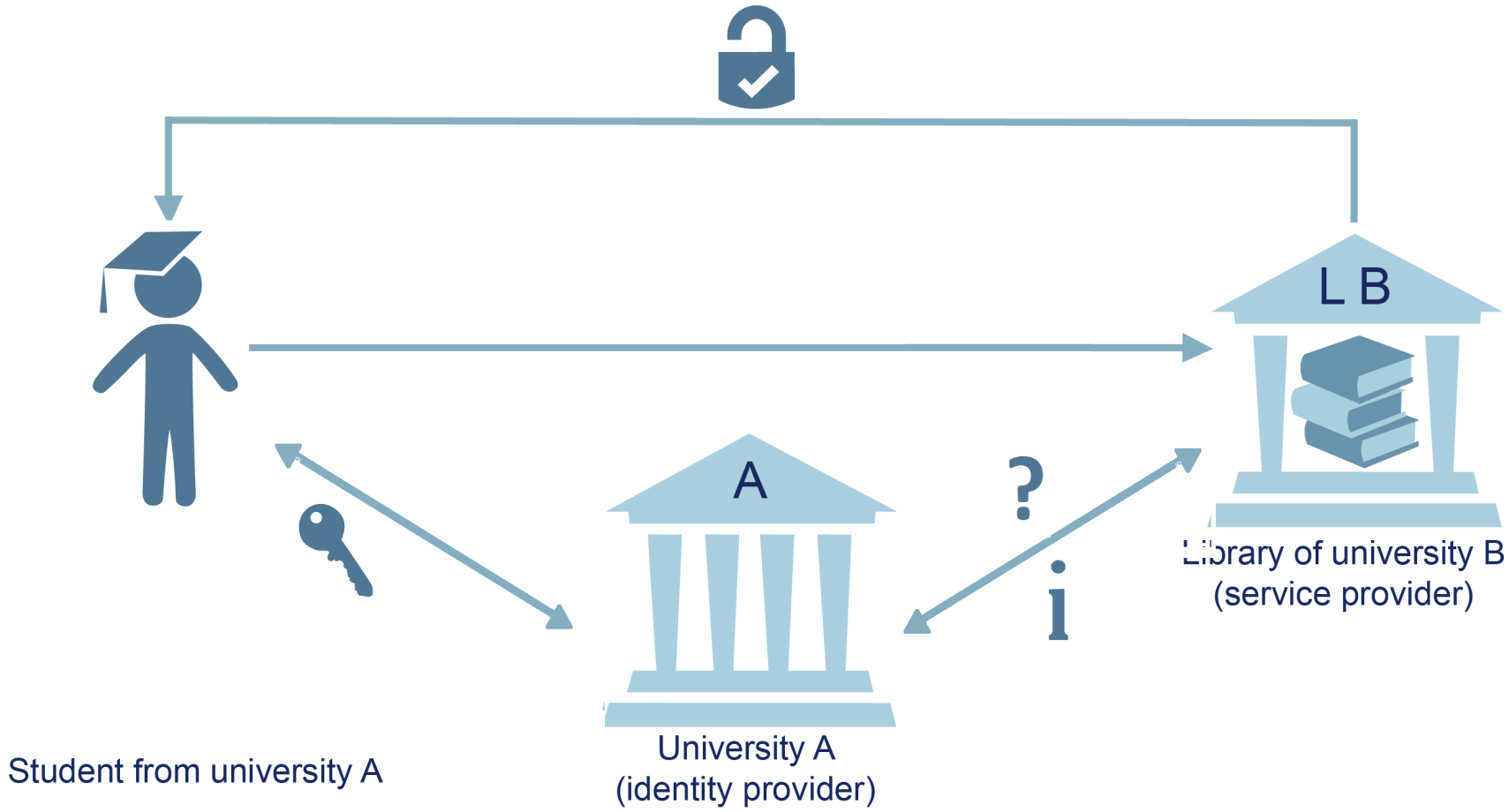
- Authentication
  - Replacing native authentication
  - Web SSO – HTTP Redirects
  - True SSO – Ticket based, e.g. Kerberos
  - Enterprise SSO - Agent
- Authorization
  - Significantly limited
  - Doesn't know application specific authorizations
  - Have you ever heard about fortress?

Federation

Federation

- SSO over the Internet
- Explicit trust and strong authentication of communicating parties
- 'In-House' authentication (Organization's IdP)
- Assertions to Service Providers, may contain
  - Roles
  - Privileges
  - User attributes
  - Authorization decissions

An example of the transmission of information between identity provider and service provider



Demo
Just-In-Time Provisioning

About Demo
Just-In-Time Provisioning

- Technologies
  - CAS – SSO Server, SAML IdP simulation
  - MidPoint – provisioning tool
  - OpenDJ – identity repository
  - OpenLDAP – target system
- Process
  - Create Identity after first login
  - Provisioning to external system – OpenLDAP
  - Create OU for user's organization
  - Assign user to groups in OpenLDAP