Open Source Identity Management

OpenAlt 2015

Evolveum

Radovan Semančík

November 2015

Ing. **Radovan Semančík**, PhD.

Software architect

Co-owner of **Evolveum** (open source company)
Architect of **midPoint** project
Apache committer (Directory API)

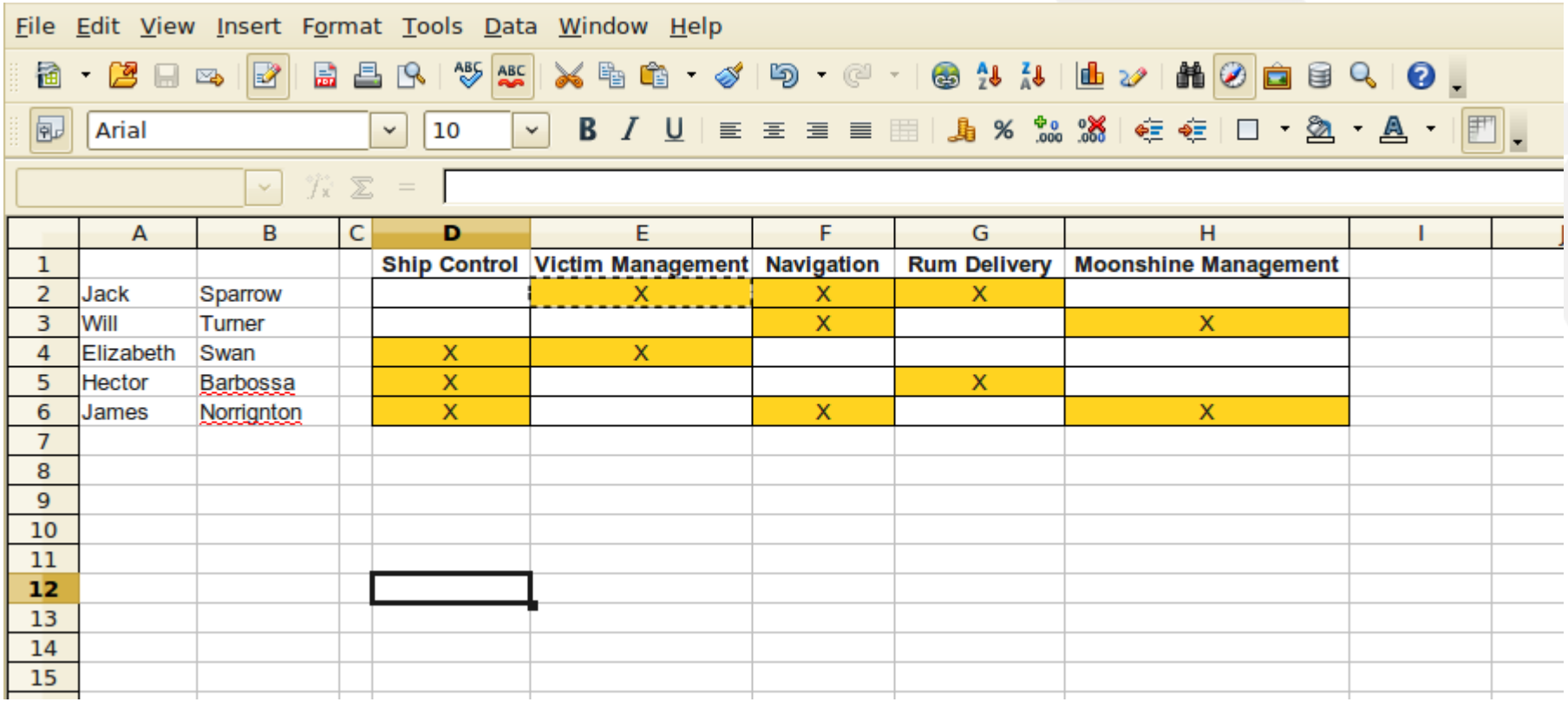
Evolveum

What is this Identity Management?

Let's start with a story ...

- Pirate Brethren, Inc.
- Fictional company
- Starts small
- Lean, efficient
- Grows quickly
- Focus on profit

Simple and easy start



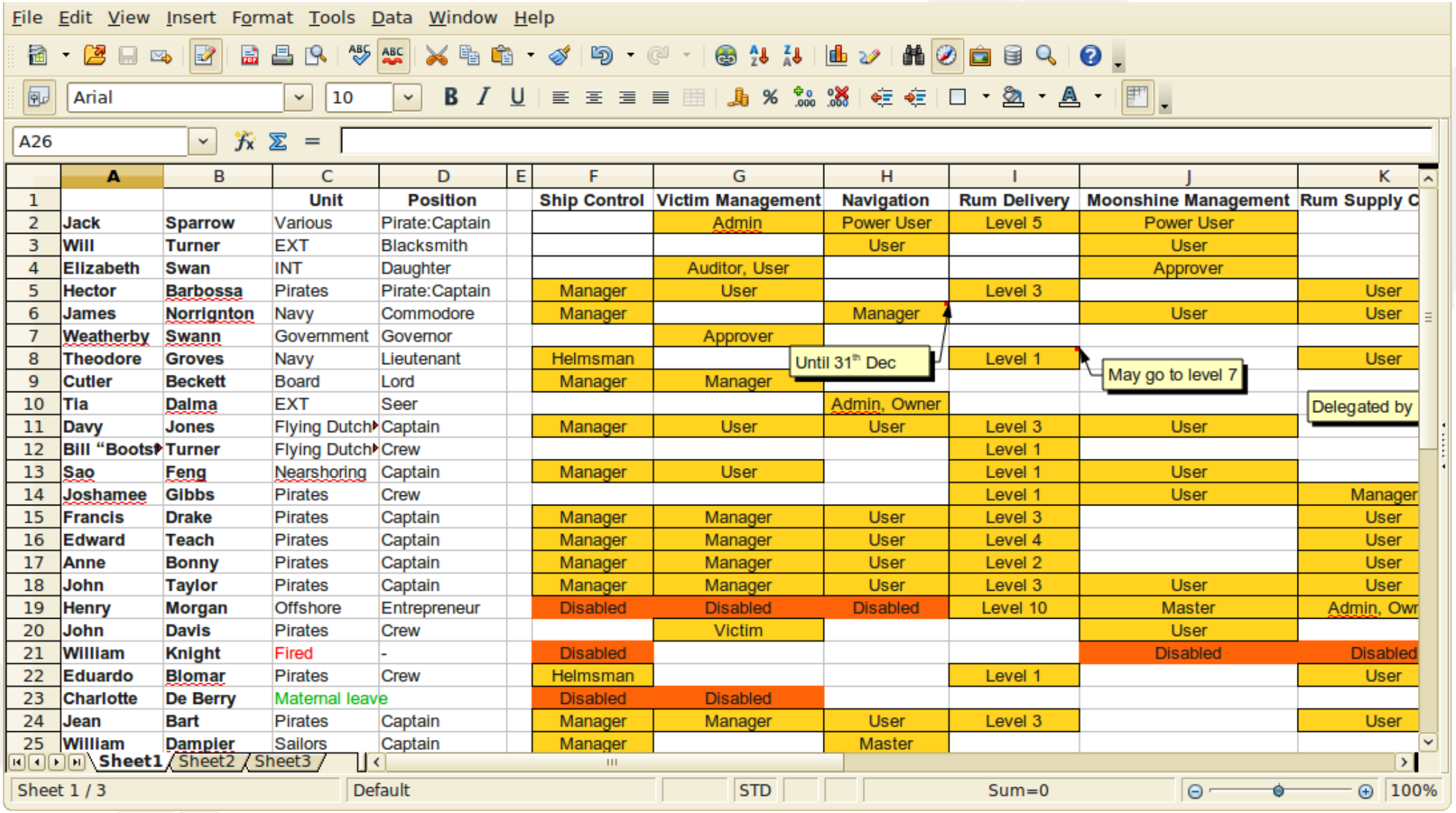
	A	B	C	D	E	F	G	H	I
1				Ship Control	Victim Management	Navigation	Rum Delivery	Moonshine Management	
2	Jack	Sparrow			X	X	X		
3	Will	Turner				X		X	
4	Elizabeth	Swan		X	X				
5	Hector	Barbossa		X			X		
6	James	Norrignton		X		X		X	
7									
8									
9									
10									
11									
12									
13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

Keeping access rights matrix in spreadsheet

Some manual work but still quite OK

Evolveum

It gets quite complex very soon ...



	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	Norrignton	Navy	Commodore		Manager		Manager		User	User
7	Weatherby	Swann	Government	Governor			Approver				
8	Theodore	Groves	Navy	Lieutenant		Helmsman			Level 1		User
9	Cutler	Beckett	Board	Lord		Manager	Manager				
10	Tia	Dalma	EXT	Seer				Admin, Owner			
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, Owr
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			

Evolveum

Login Nightmares

Shippin' DeLuxe v99.02

Login: mjones

Password:

Forgot password?

NaviGATE+

Username: p0054358

Password:

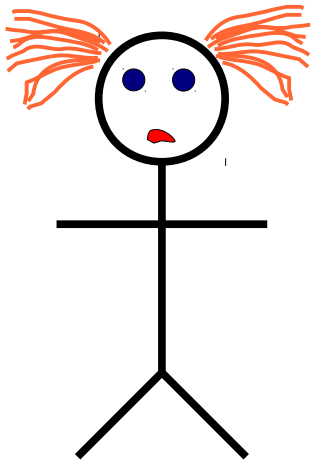
```
Login: marry
Password:
```

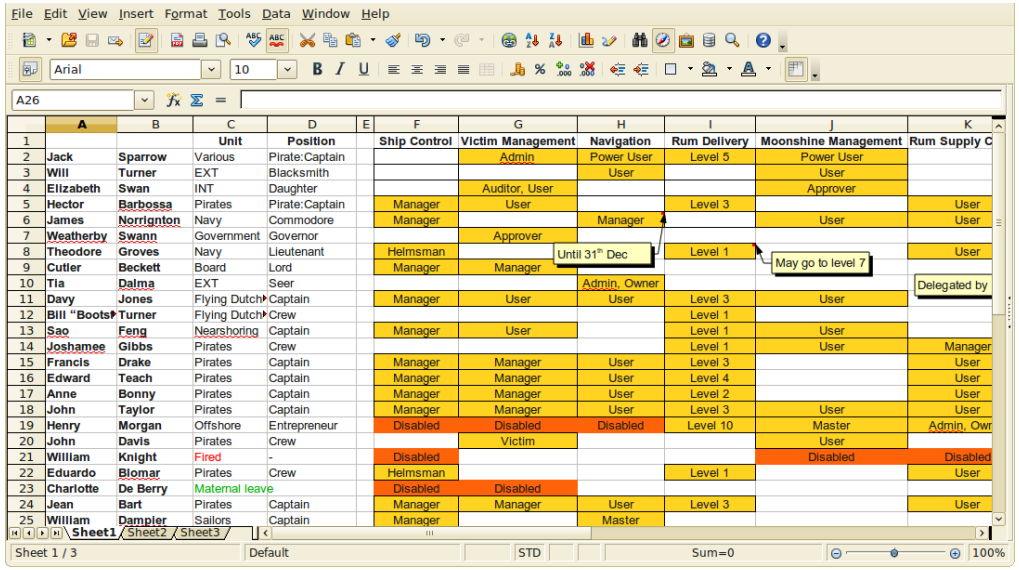
CrashSoft Woknous

Realm: PIRACY

Login: jones3

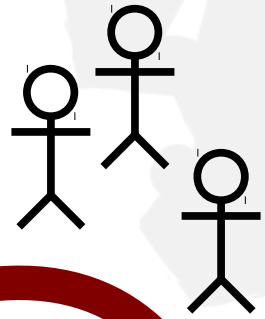
Password:

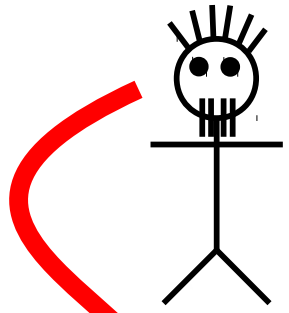




	A	B	C	D	E	F	G	H	I	J	K
1			Unit	Position		Ship Control	Victim Management	Navigation	Rum Delivery	Moonshine Management	Rum Supply C
2	Jack	Sparrow	Various	Pirate:Captain			Admin	Power User	Level 5	Power User	
3	Will	Turner	EXT	Blacksmith				User		User	
4	Elizabeth	Swan	INT	Daughter			Auditor, User			Approver	
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	May go to level 7	User
9	Cutler	Beckett	Board	Lord		Manager	Manager				
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, Owr
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			

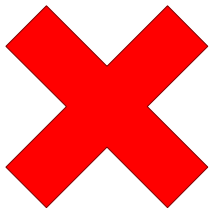
Policy





untracked changes

manual synchronization (unreliable, slow, costly)



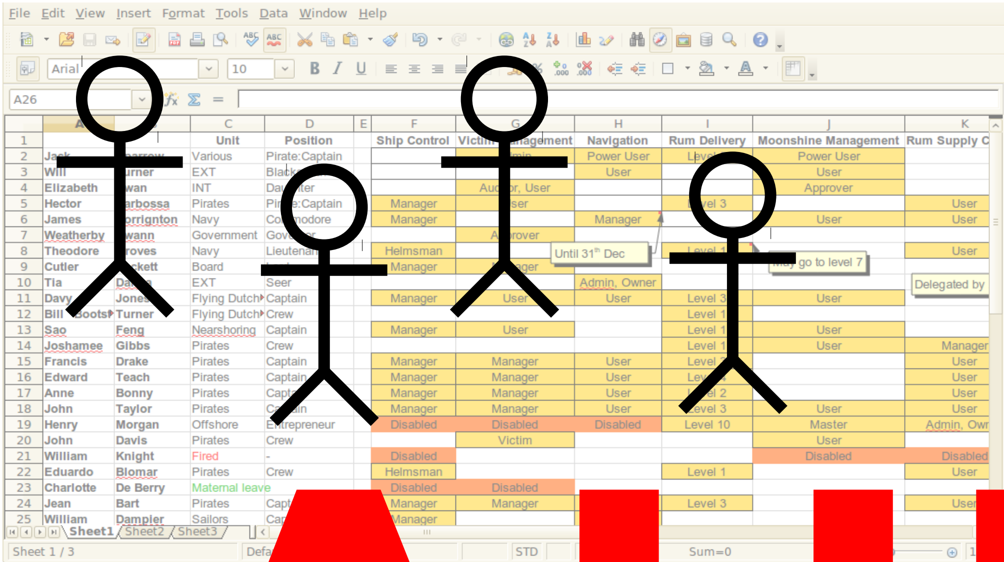
no feedback

Reality

```
# LDAPv3
# base <dc=example,dc=com> with scope subtree
# filter: (entryUUID=48b2295e-c131-4300-835a-fa85c863233e)
# requesting: ALL
#


# jack, people, example.com
dn: uid=jack,ou=people,dc=example,dc=com
mail: jack2@blackpearl.com
givenName: Jack
objectClass: person
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: top
uid: jack
cn: cpt. Jack Sparrow
sn: Sparrow
```

Evolveum



AUDIT

VERY COSTLY

… and it has to be repeated …

```
LDAPv3
...ample,dc... with scop...tree
...(entryUUID=...95e-c131-4...35a-fa85c863233e)
# requesting: ALL
#


# jack, people, example.com
dn: uid=jack,ou=people,dc=example,dc=com
mail: jack2@blackpearl.com
givenName: Jack
objectClass: person
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: top
uid: jack
cn: cpt. Jack Sparrow
sn: Sparrow
```

Evolveum

Call Center Goes Crazy

Access request

Password reset

Password reset

Password reset

Password reset

Password reset

Password reset

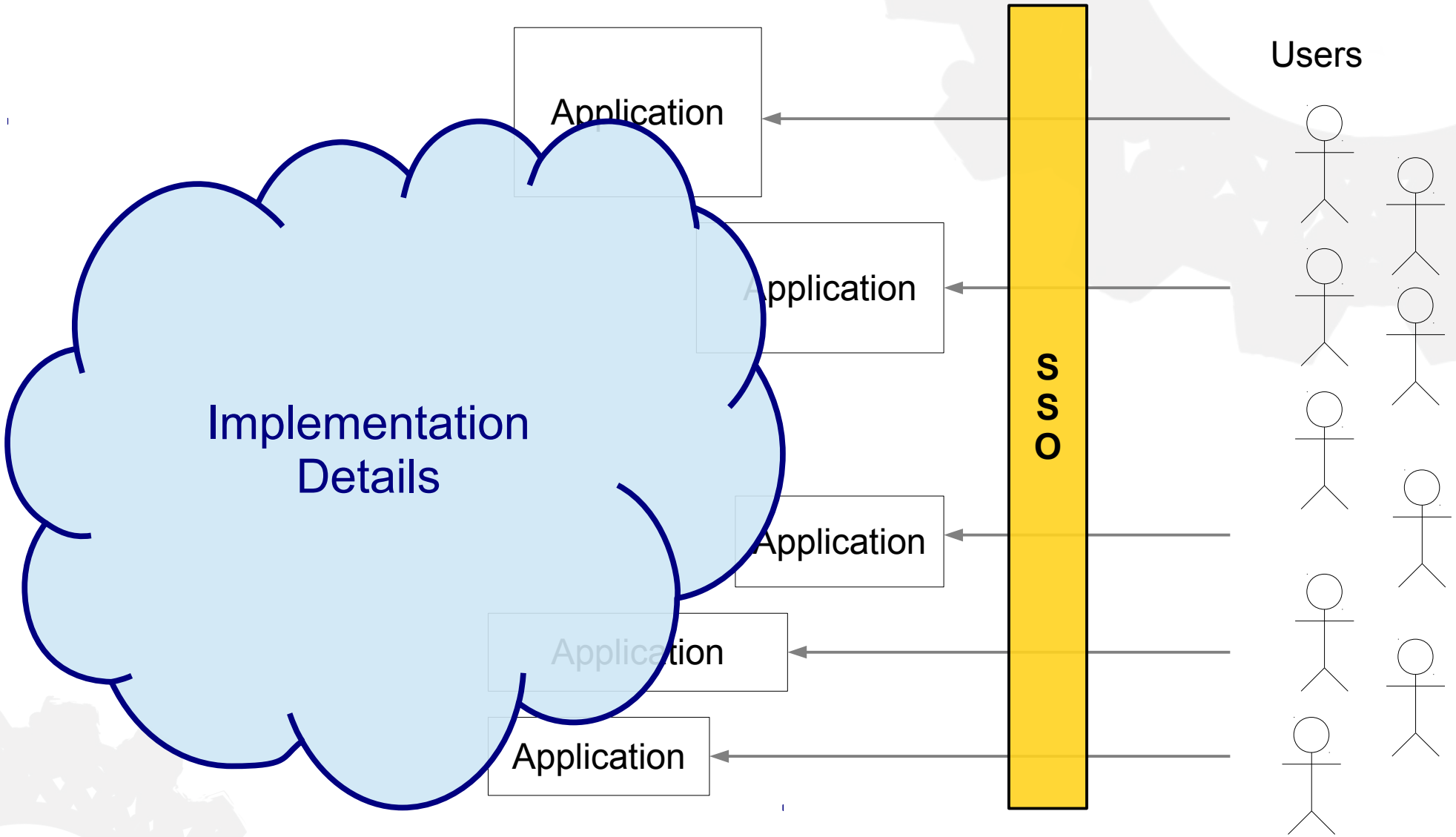
Access request

Password reset

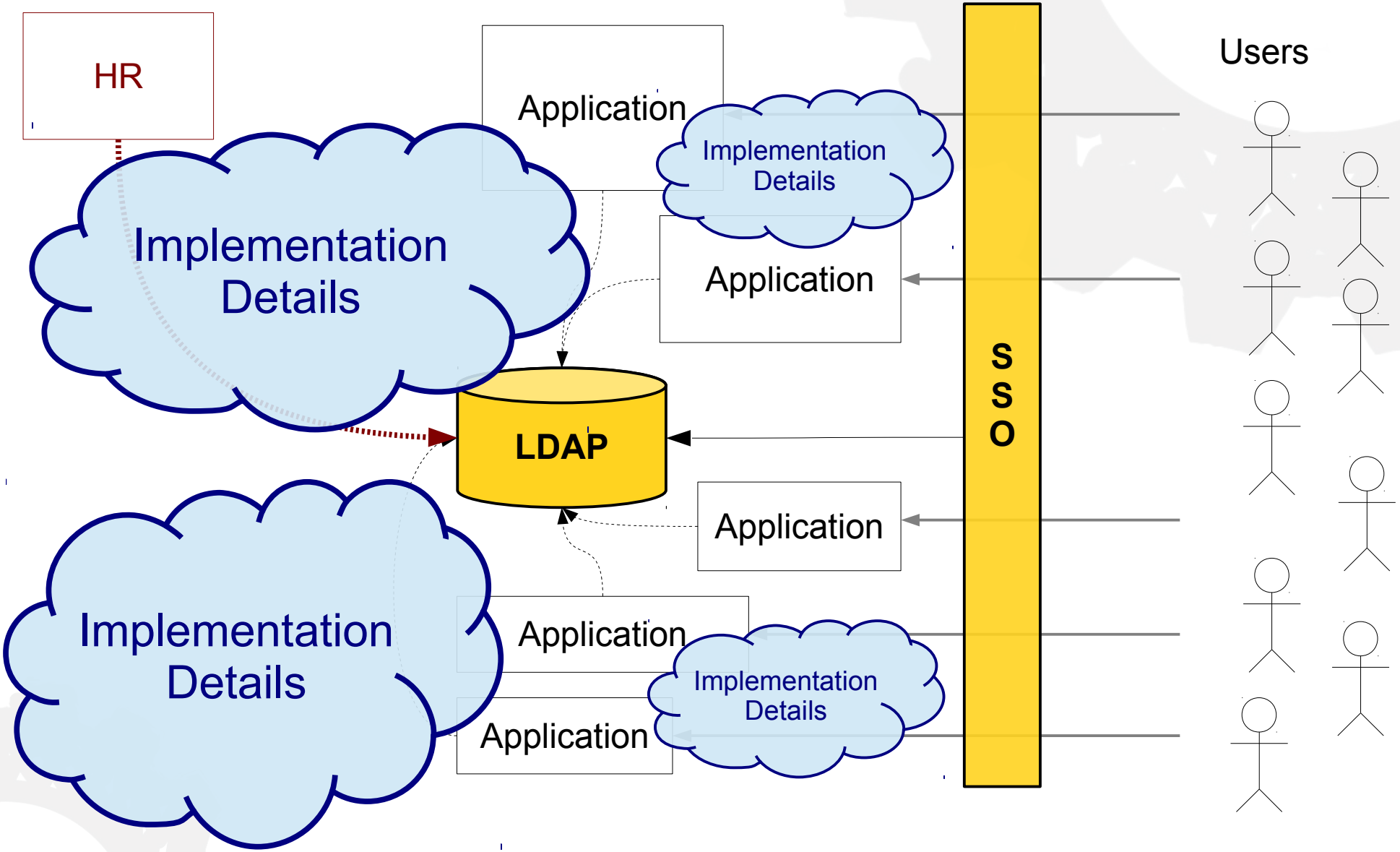
Let's do this IAM* thing.
Everybody is doing that.

*) Identity and Access Management

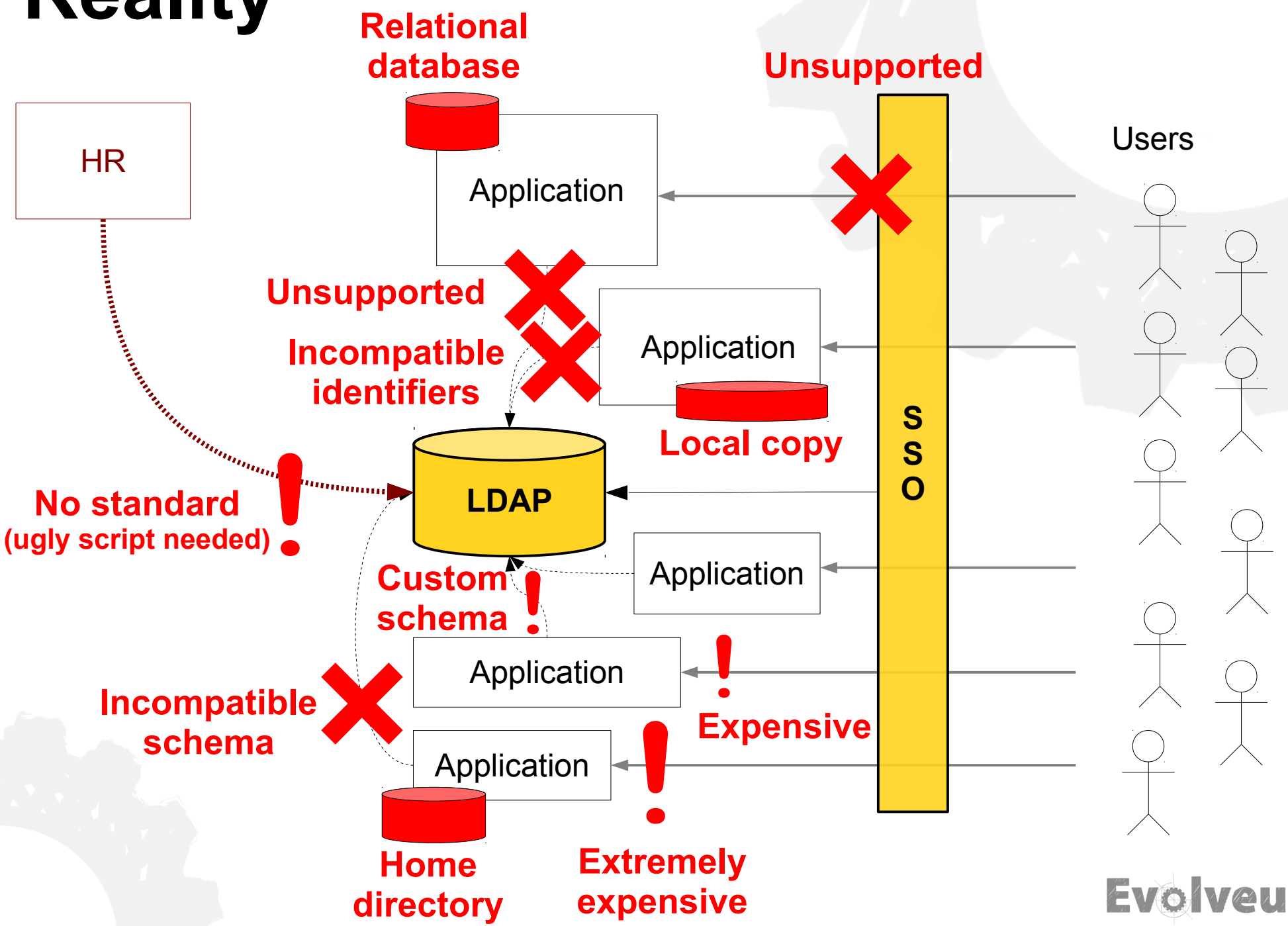
Manager's View



High Level Architect's View



Reality



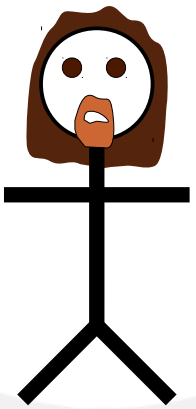
Evolveum

“Single directory” approach is not going to work

… and this has been known since 2006 (at least)

What are we going to do now?

DO NOT PANIC!

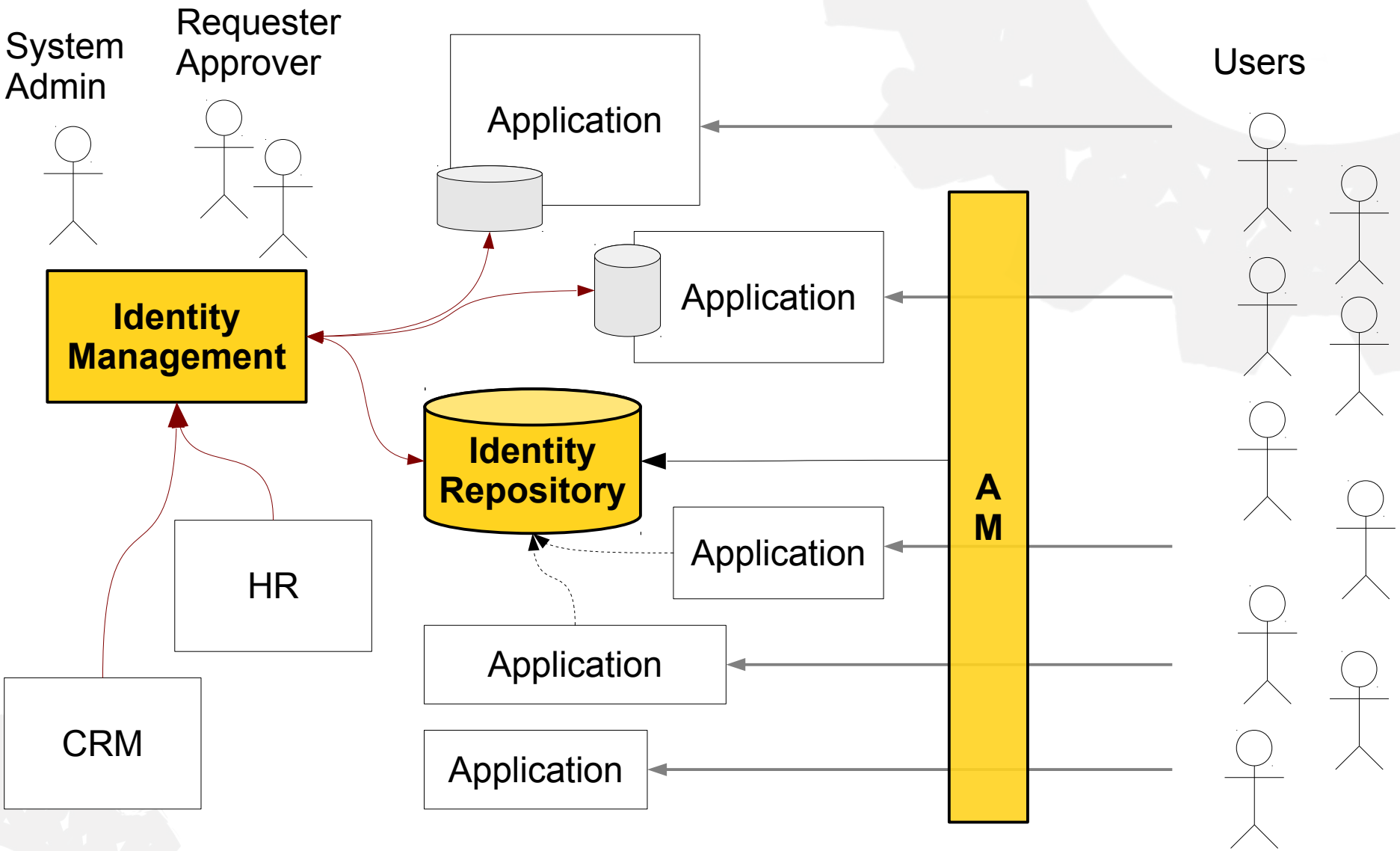


SSO is what you think you **want**

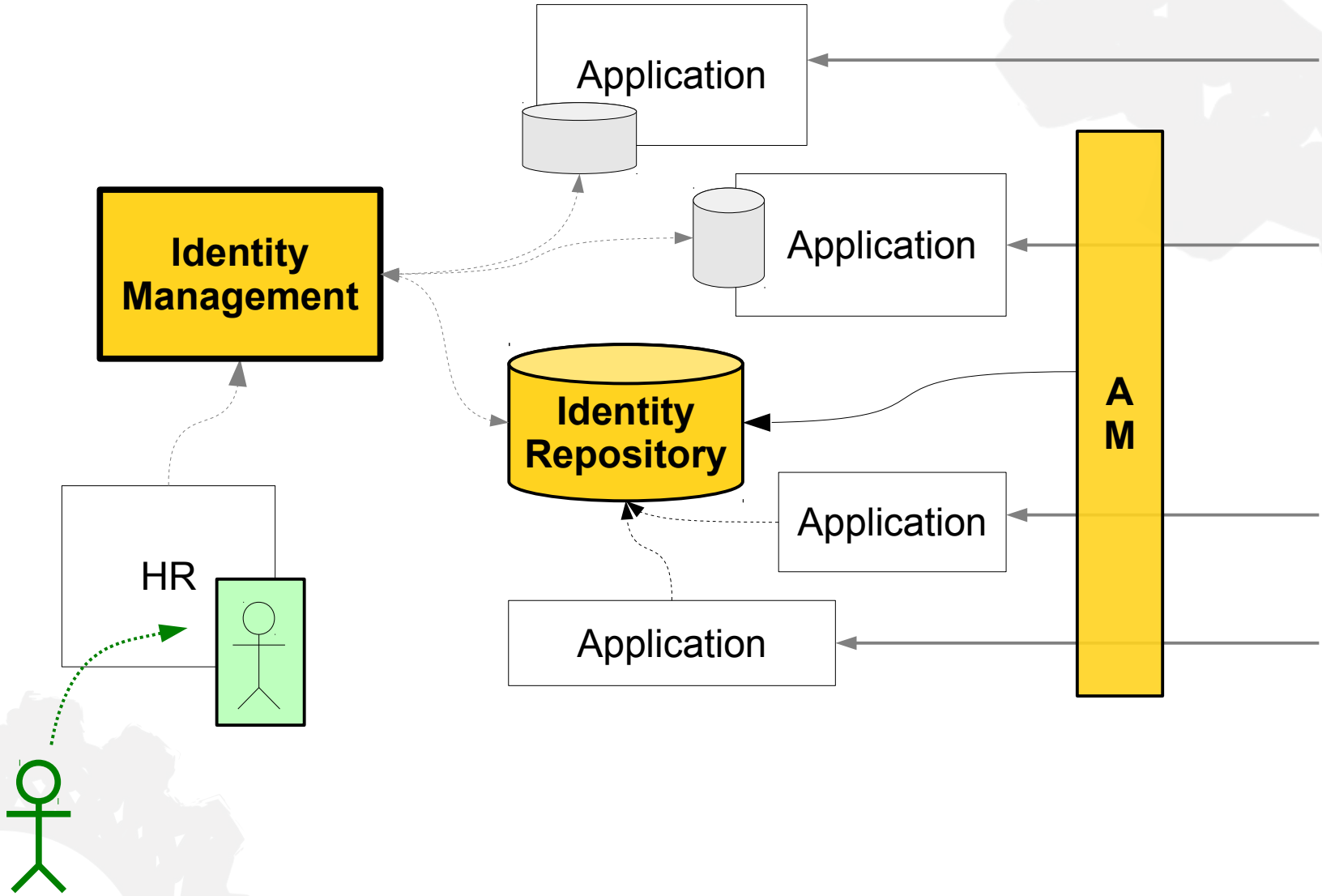
IDM is what you really **need**

What is this Identity Management (IDM) thing, again?

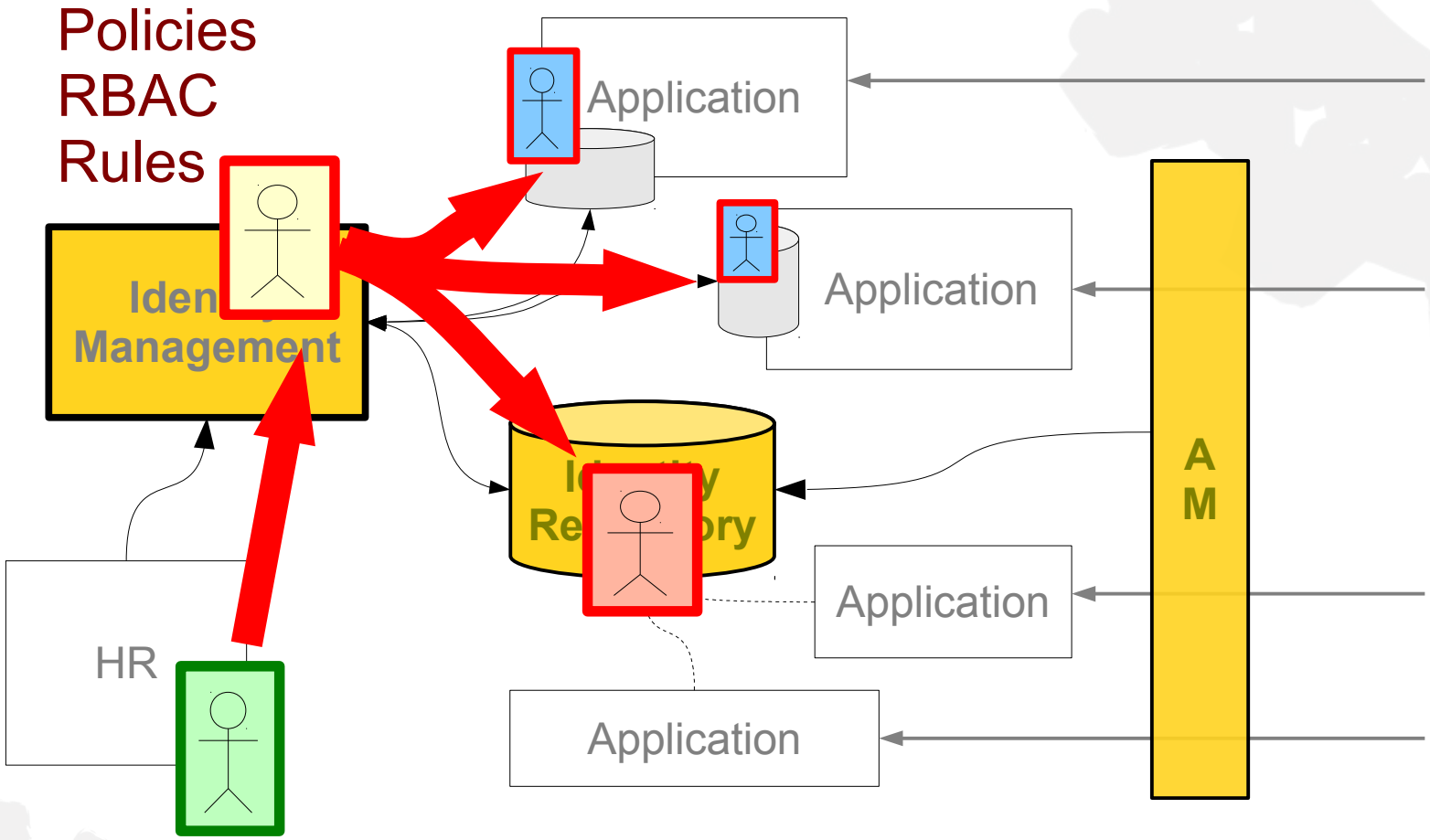
Identity and Access Management



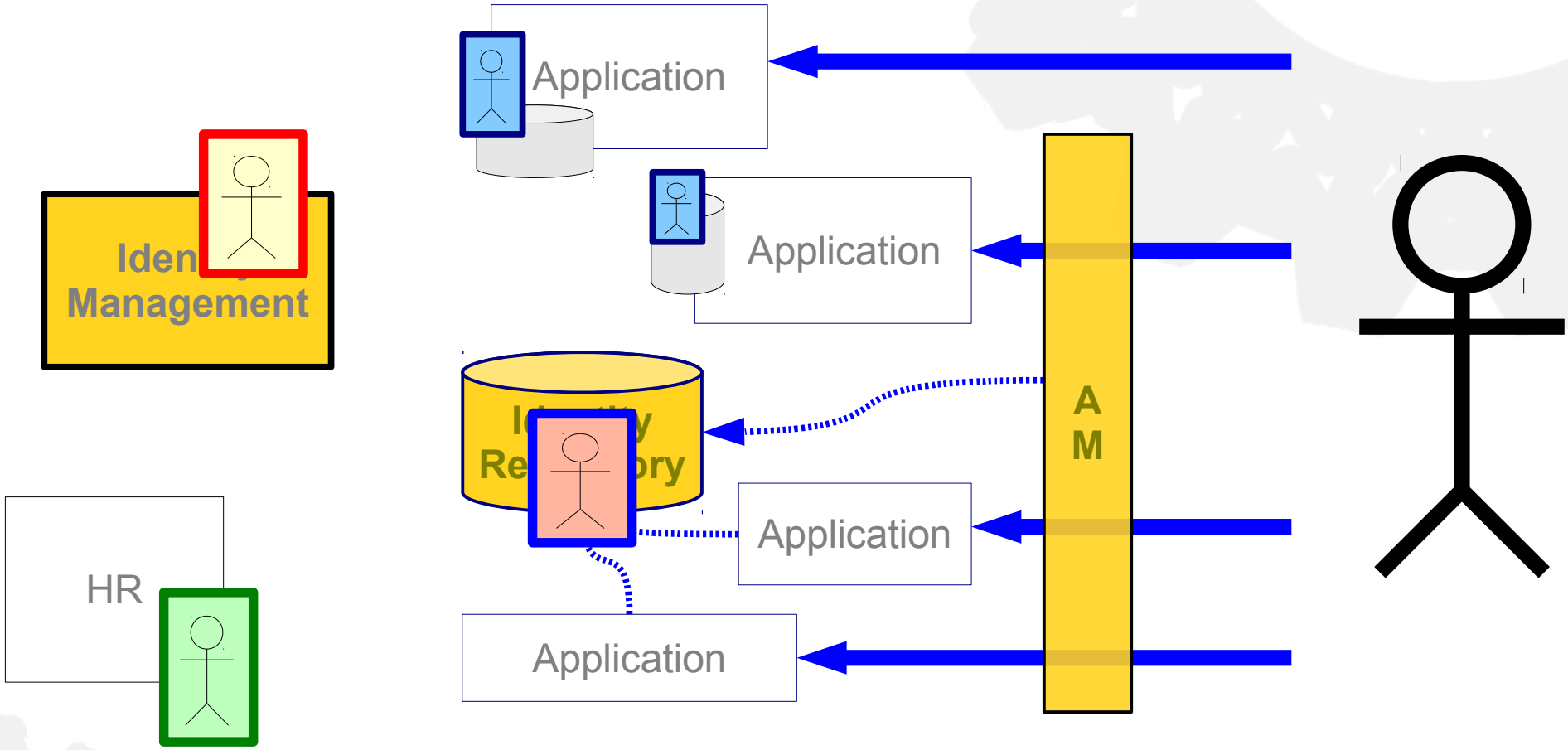
How IDM works?



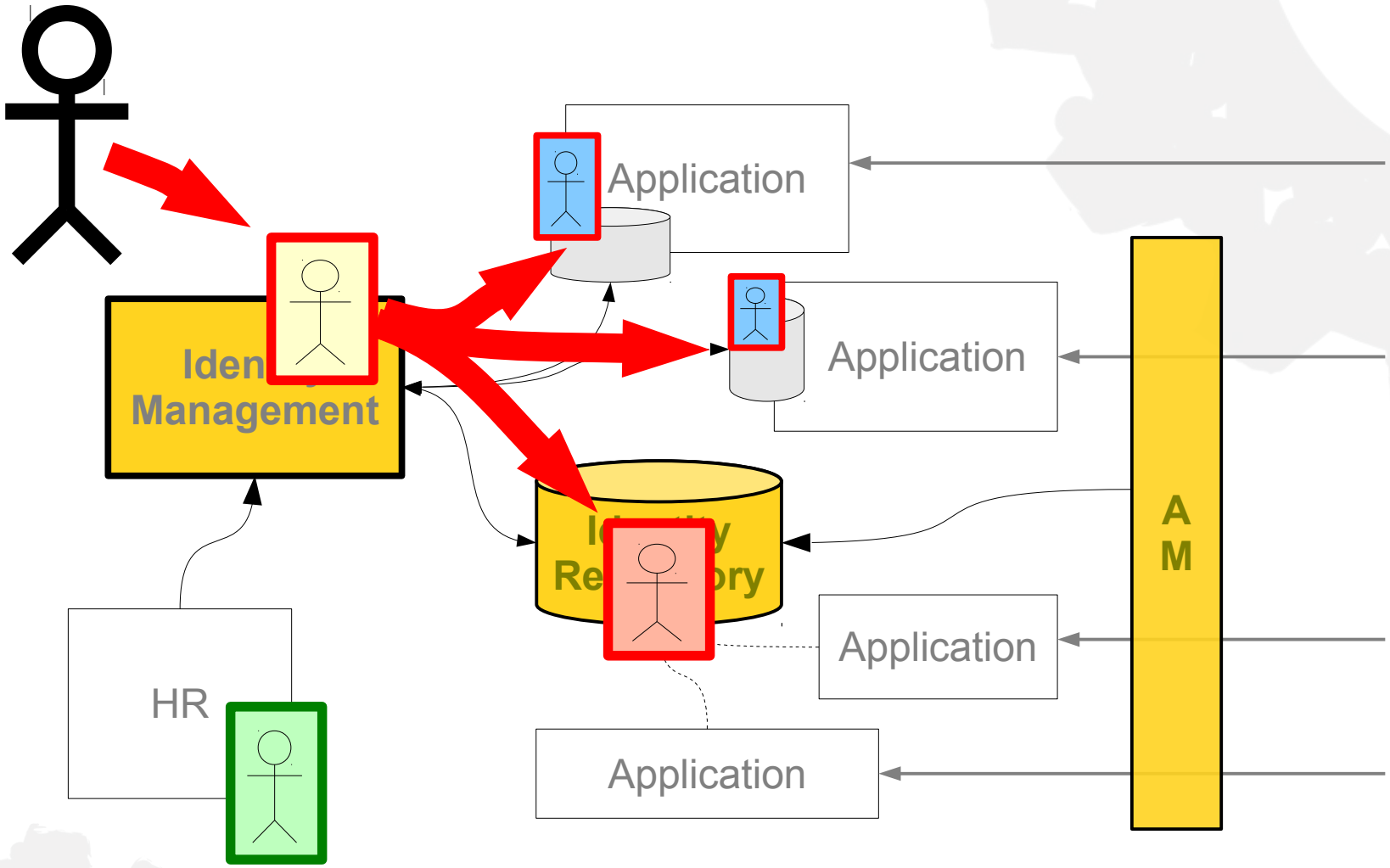
Automatic user provisioning



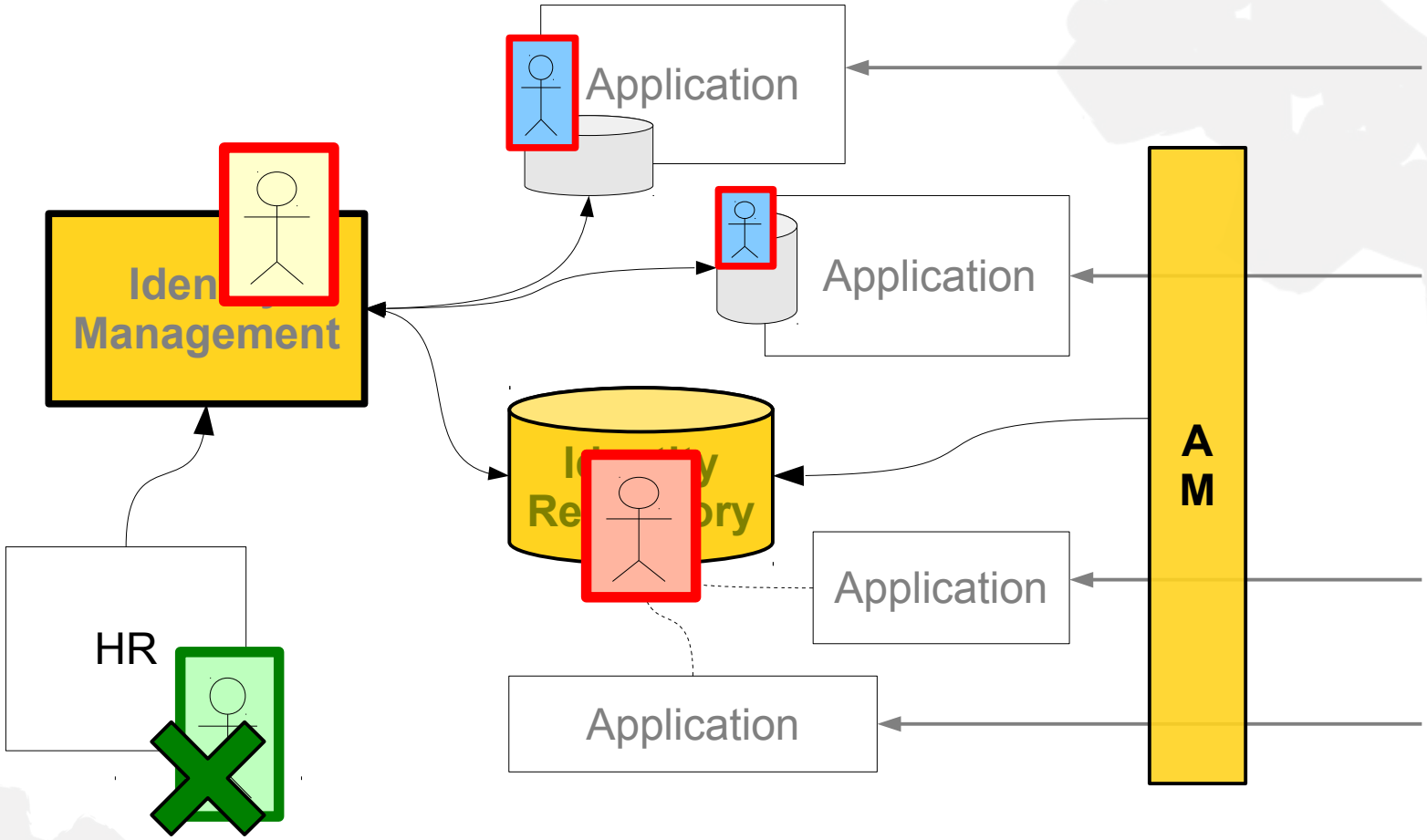
Business As Usual



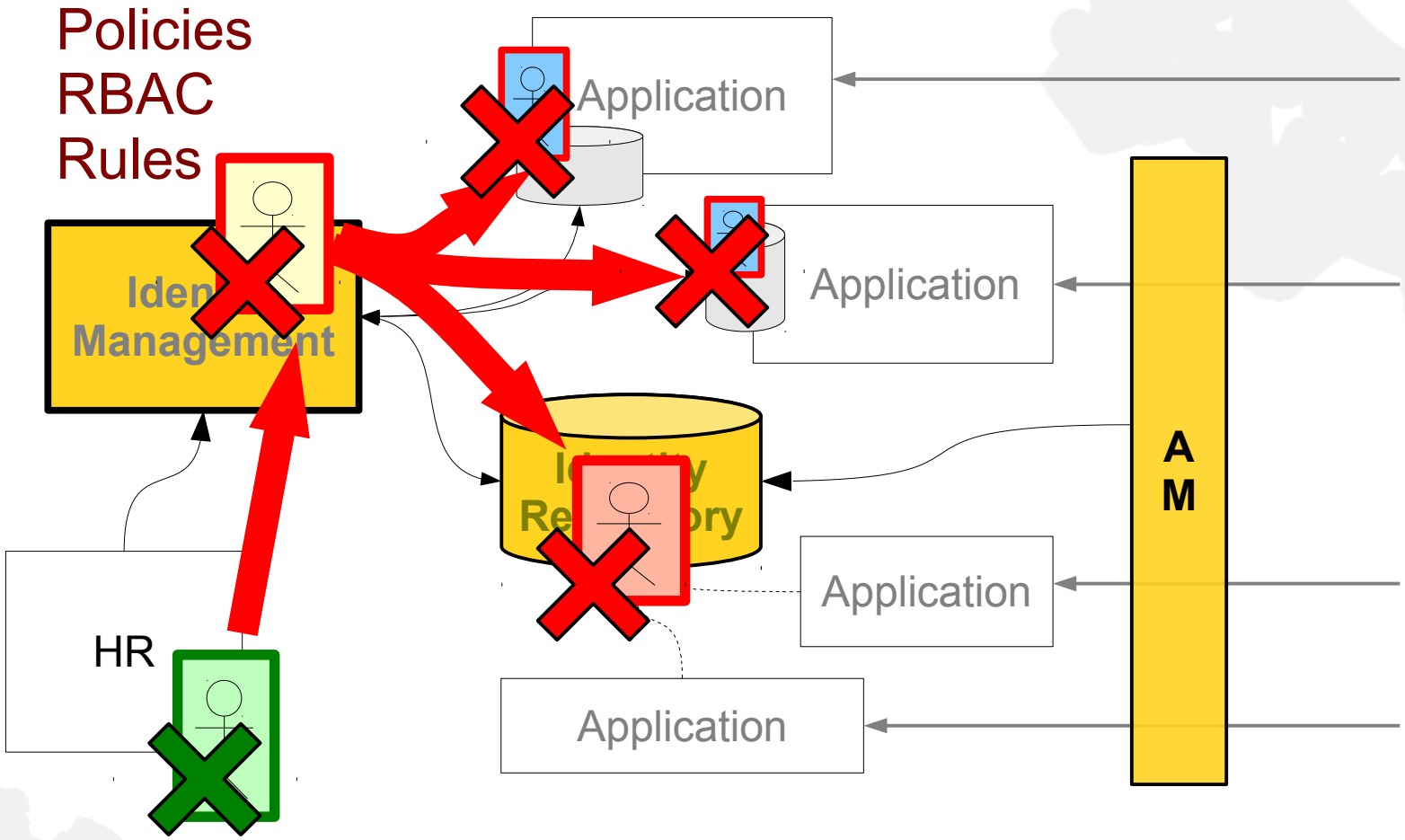
Password reset (self-service)



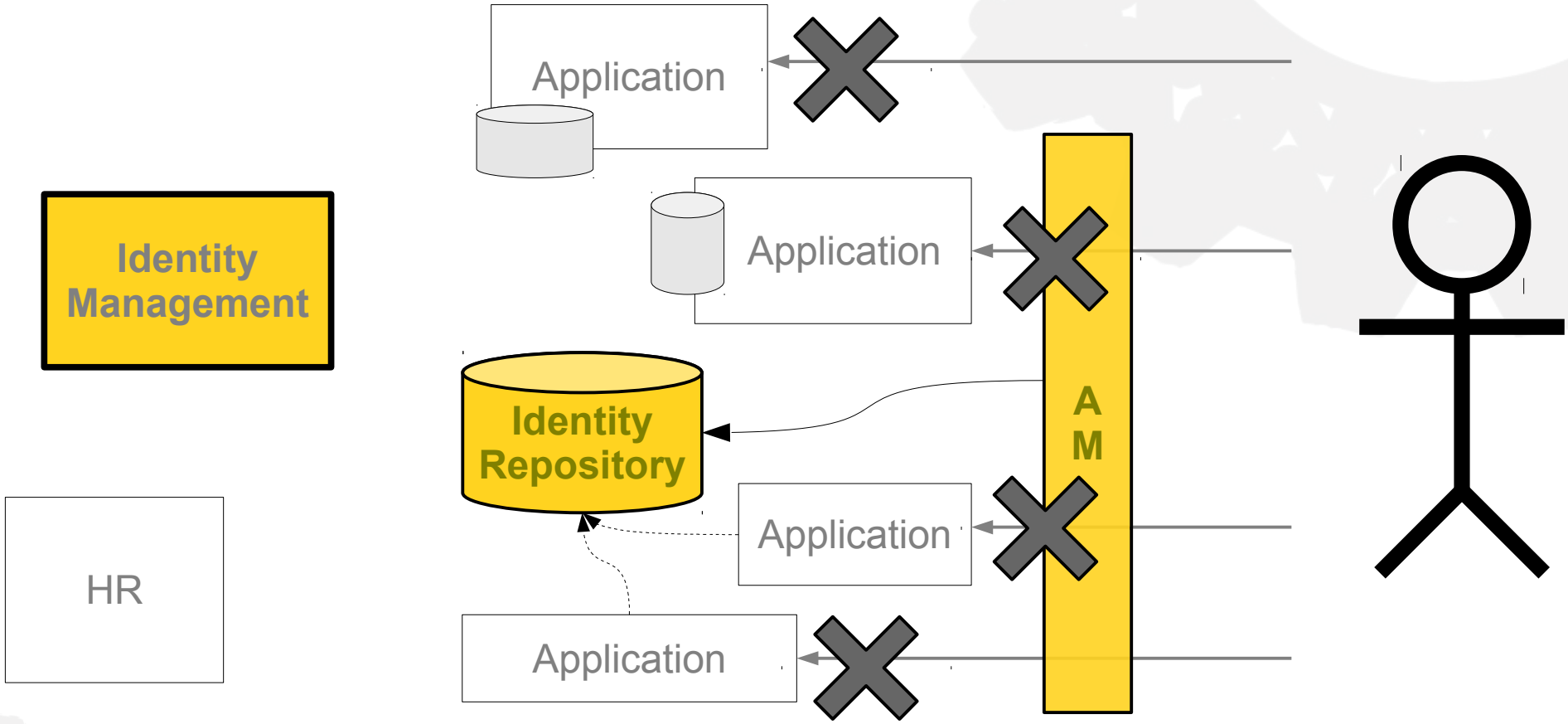
Employee Leaves Company



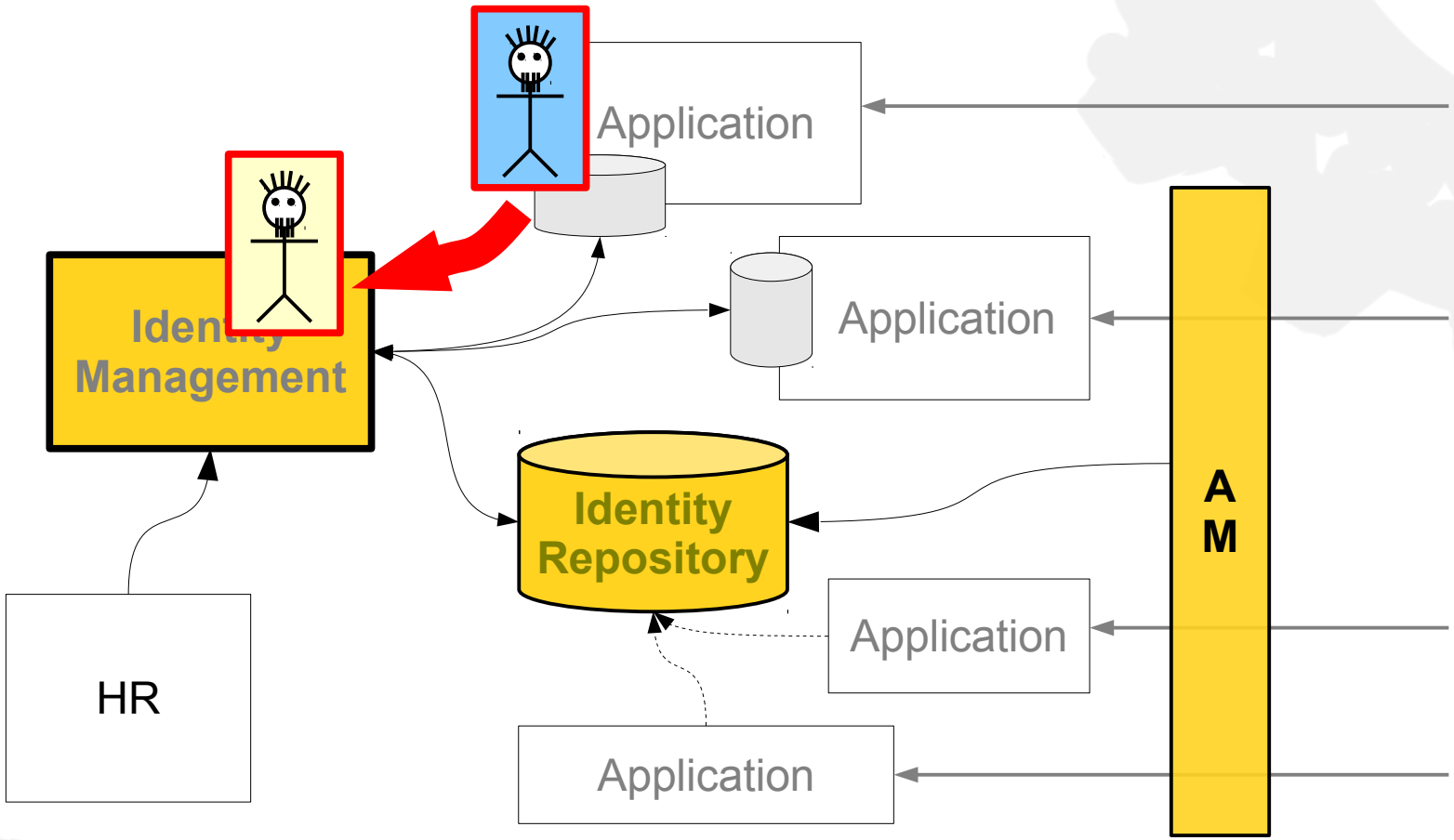
Automatic user deprovisioning



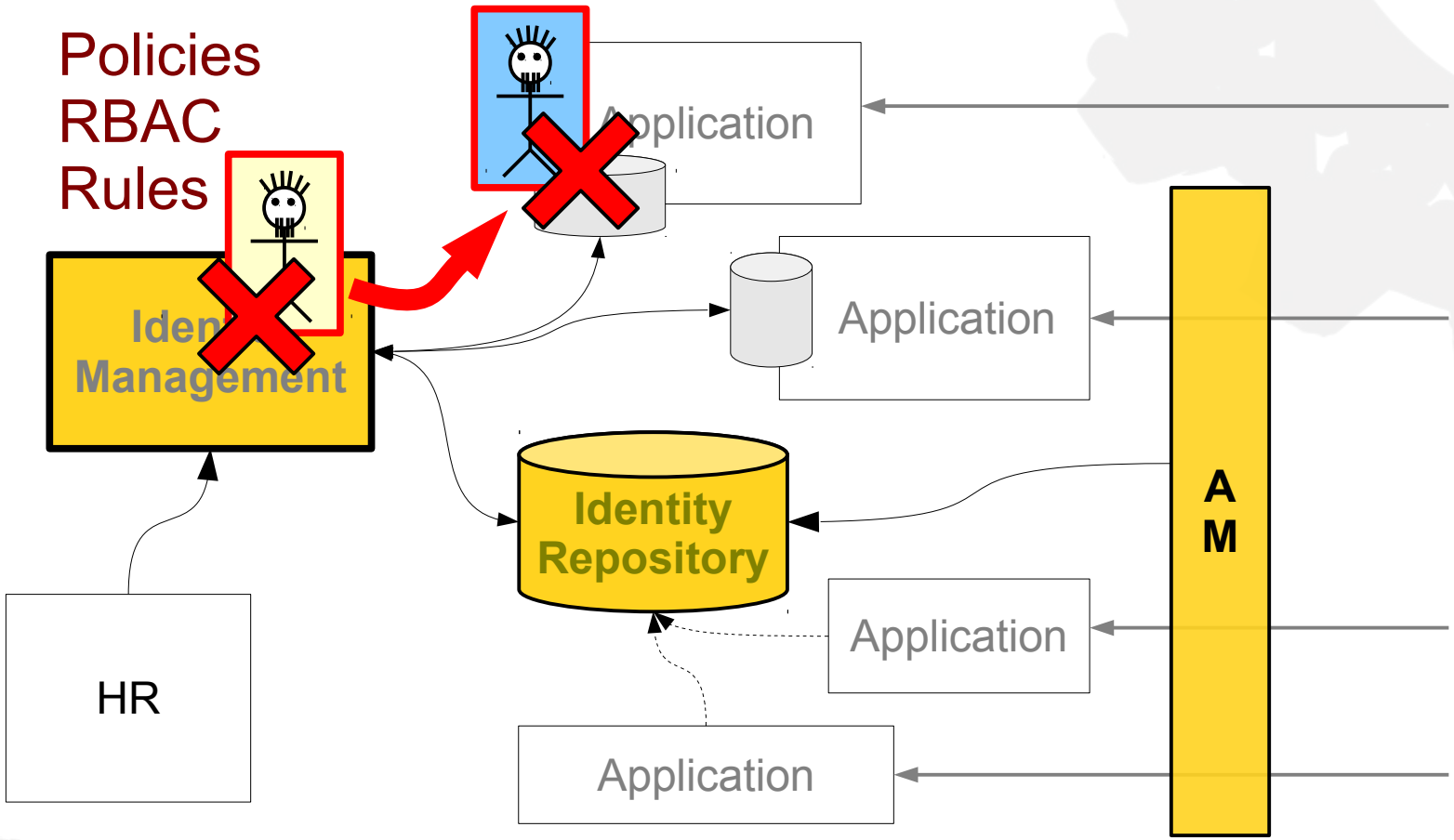
Business As Usual



Bidirectional Synchronization



Policy enforcement



What Identity Management does?

- Provisioning
- Synchronization
- Self-service
- Password management
- Credentials distribution (SSH, X.509)
- RBAC
- Organizational structure
- Entitlement management
- Identifier management
- Data mapping
- Segregation of duties
- Workflow
- Notifications
- Auditing
- Reporting
- Governance
- ...

Who needs Identity Management?

IDM Rule of the Thumb:

- < 100 identities: you are fine with manual work
- 100 – 1K identities: you might need it
- 1K - 10K identities: you need it
- > 10K identities: you **desperately** need it!

This IDM looks like the best thing since the sliced bread. What's the catch?

This IDM looks like the best thing since the sliced bread.
What's the catch?

The commercial IDM products are expensive.

This IDM looks like the best thing since the sliced bread.
What's the catch?

The commercial IDM products are expensive.

Very, very expensive.

Open Source to the Rescue

There was no practical FOSS solution until 2010

(Sun Identity Manager was the king)

2010-2011: Syncope, OpenIDM, midPoint, ...

(that was the time when Oracle acquired Sun)

Now there are two leading open source* IDMs:

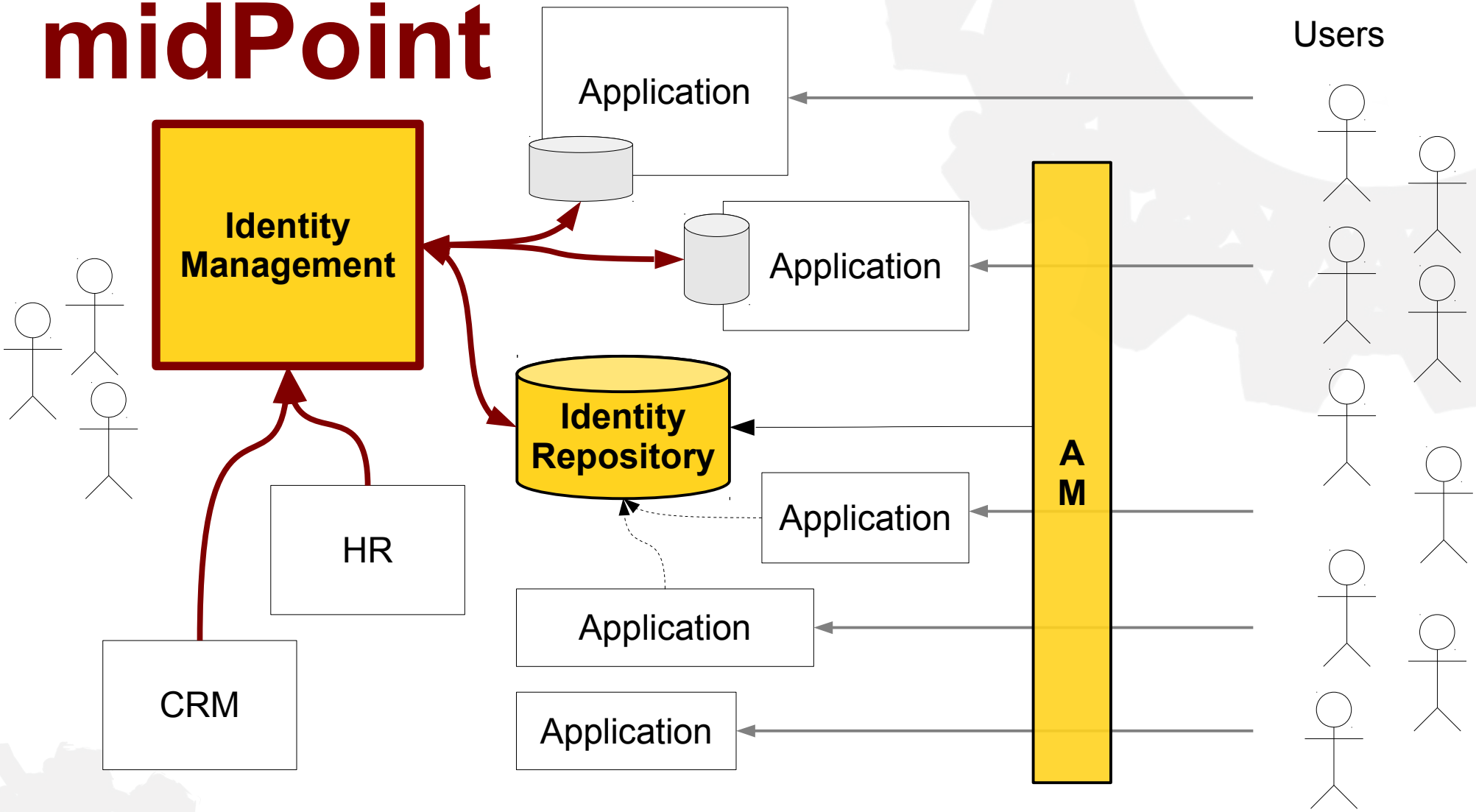
- Apache Syncope
- Evolveum midPoint

*) by “open source” I mean both license and practice

Evolveum midPoint?

Evolveum

midPoint



Evolveum

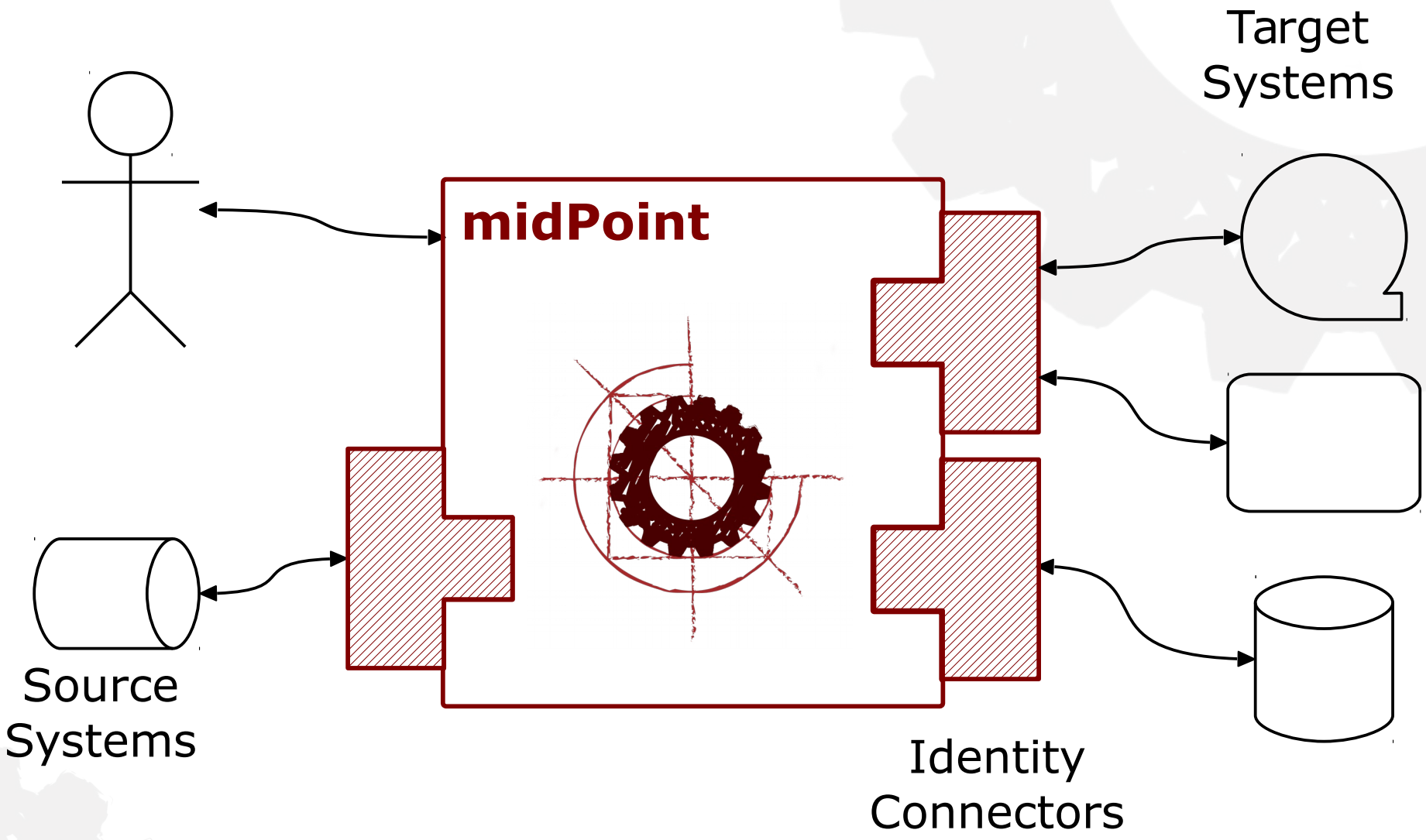
The midPoint Story

- Started 2010-2011 (5 years, 14 releases)
- Github, Apache 2.0 License
- ~500K lines of code (Java)
- State-of-the-art IDM features

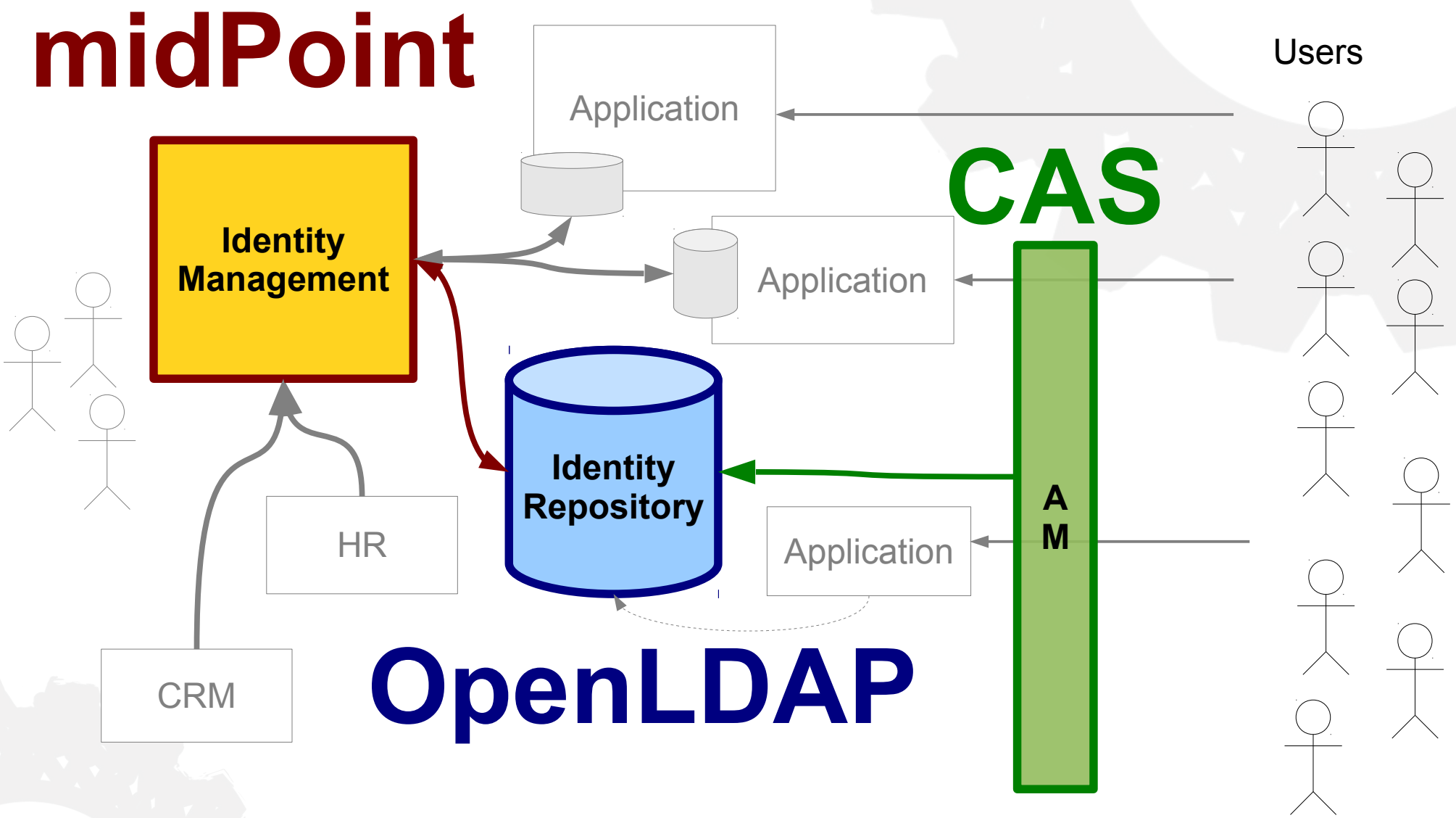
Conditions Provisioning Management Schema Extensibility
Expressions Segregation of duties Password reset
RBAC Synchronization Policy Organizational structure
Consistency Workflow Entitlements Connectors HA
Web UI Governance
Audit Authorization Localization Notifications
Scripting Self-service Data mapping REST Identifiers
Parametric roles Delegated administration
Bulk actions

Evolveum

MidPoint Big Picture



Complete Open Source Solution

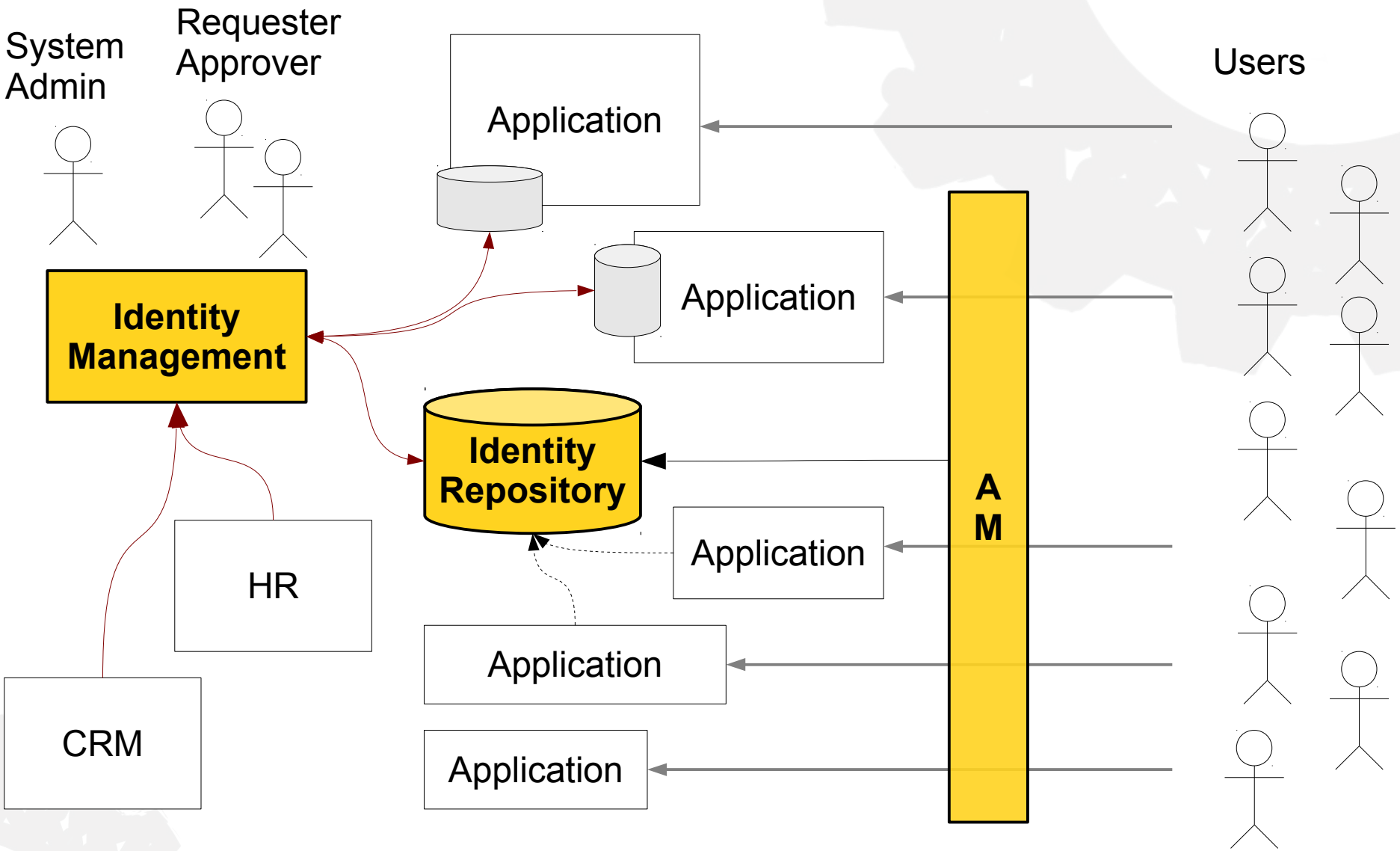


Evolveum

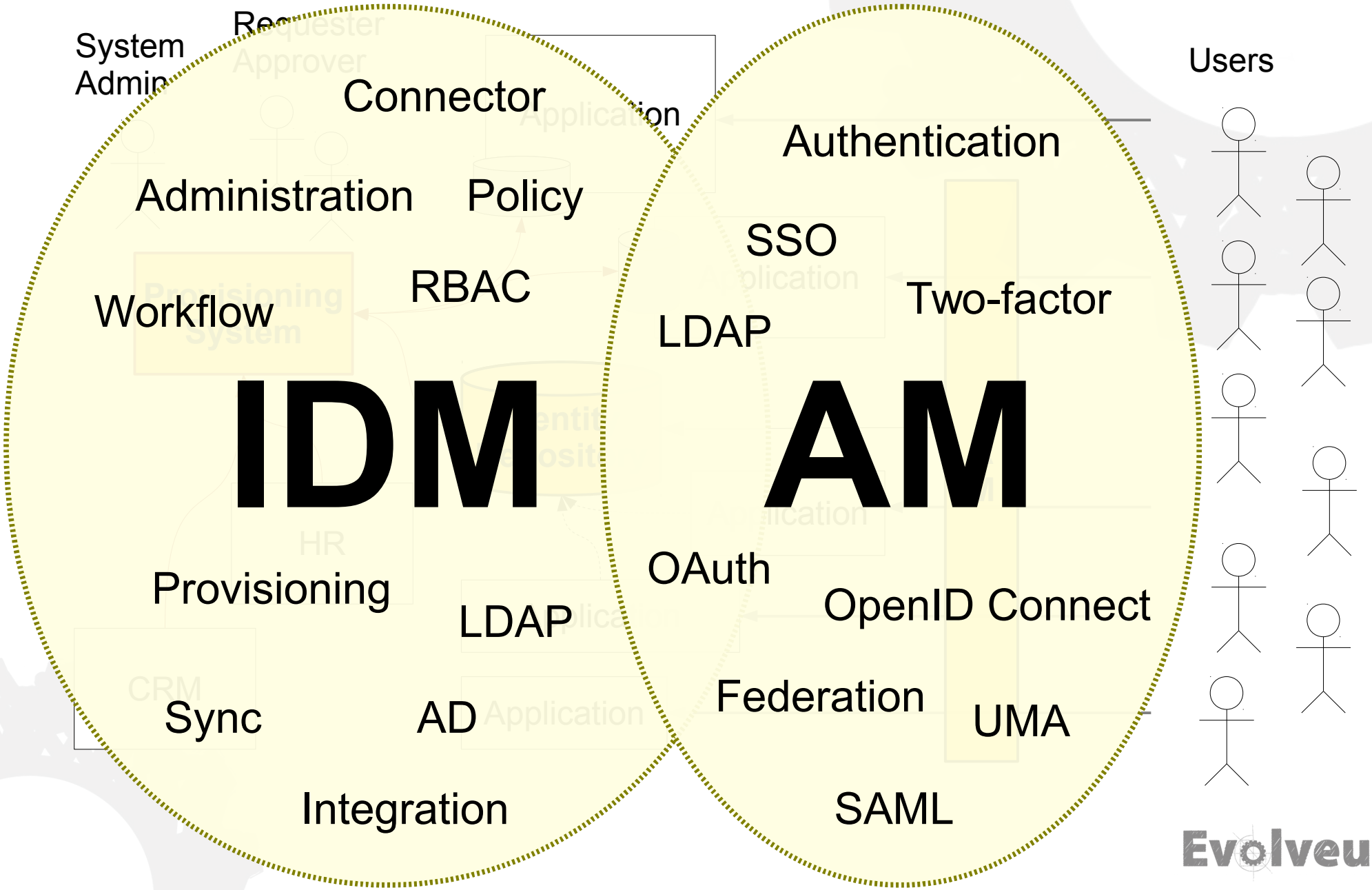
Conclusion

Evolveum

Identity and Access Management



IAM Letter Soup



Evolveum

Access Management

- Authentication
- Single Sign-On (SSO)

- Quite expensive

What people want

Identity Management

- Provisioning
- RBAC
- Synchronization
- Password management
- Self-service
- … and much more

- Cost reduction

What people need

Access Management

- Authentication
- Single Sign-On (SSO)

- Quite expensive

What people want

Identity Management

- Provisioning
- RBAC
- Synchronization
- Password management
- Self-service
- … and much more

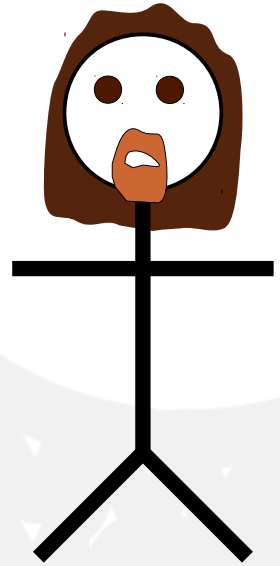
- Cost reduction

What people need

Questions and Answers

Evolveum

Thank You



Radovan Semančík

www.evolveum.com

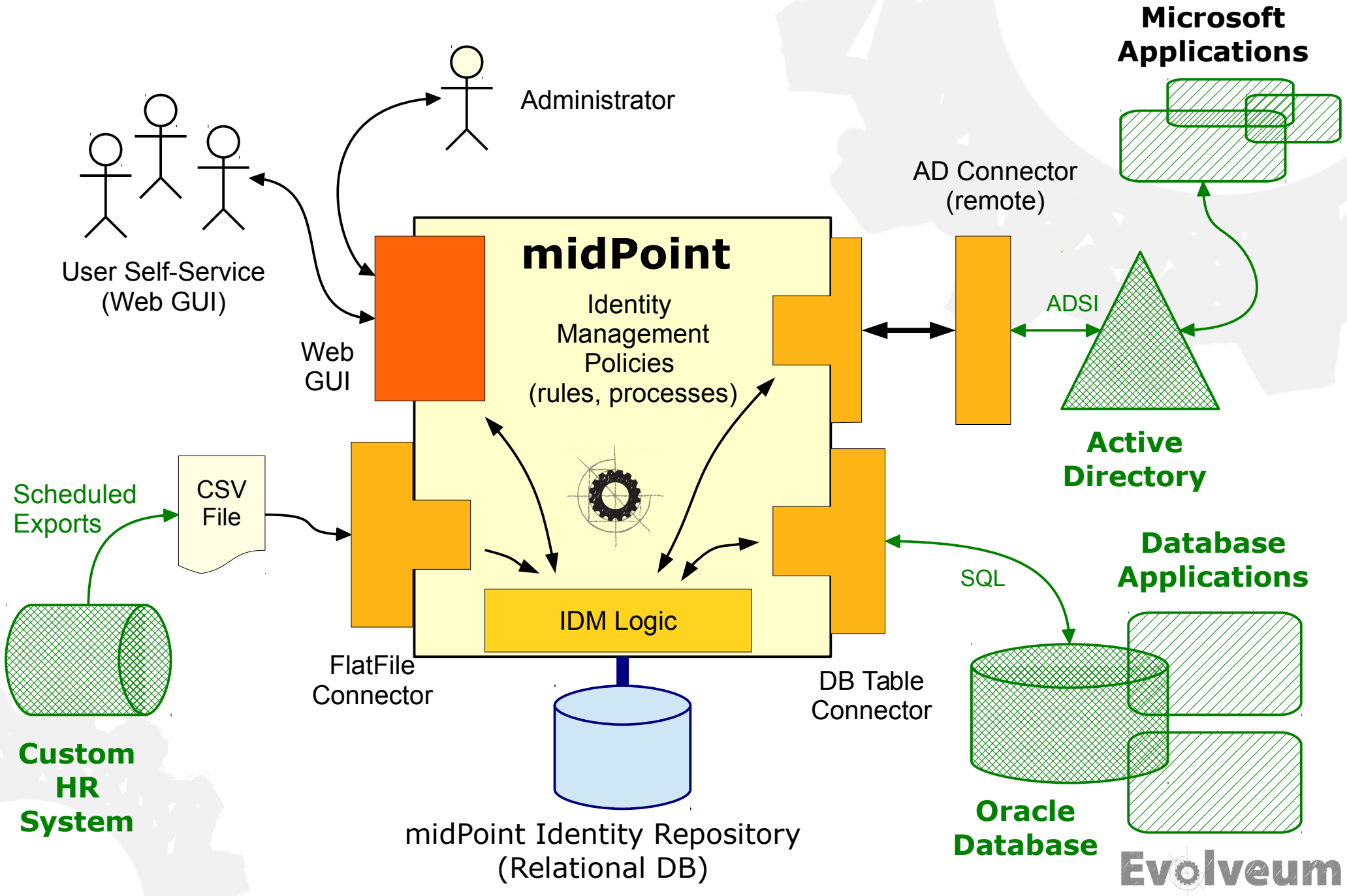
Extra Slides

Evolveum

(Much) More Information

- midPoint Wiki
  - https://wiki.evolveum.com/display/midPoint/Home
- Architecture and Design (in Wiki)
  - Wiki pages under [Architecture and Design] page
  - “Live” architecture documentation
  - Includes UML diagrams
  - We try to keep it (reasonably) up to date
- midPoint Mailing List

Example midPoint Deployment Architecture



Identity Connectors

- Common Identity Connector Framework
  - Sun Identity Connector Framework → **ConnId**
- Compatible connectors
  - AD, DB Table, DB2, MySQL, Oracle, RACF, Solaris, SPML, VMS, FlatFile, XML, Solaris, SAP, ...
  - LDAP: OpenLDAP, 389ds, OpenDJ, eDirectory, Active Directory
  - CSV file, Office365, SAS, GitLab, Lotus, LifeRay

Live Demo

`http://demo.evolveum.com/`

Documentation: search for “Live demo” in wiki.evolveum.com