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

Keeping access rights matrix in spreadsheet

Some manual work but still quite OK

Evolveum

It gets quite complex very soon ...

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: [   ]

Evolveum

Policy

manual synchronization
(unreliable, slow, costly)

untracked
changes

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
```

Spreadsheet (top-left):

File Edit View Insert Format Tools Data Window Help

Arial   10   B I U

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	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			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		User	User
19	Henry	Morgan	Offshore	Entrepreneur		Disabled	Disabled	Disabled	Level 10	Master	Admin, Own
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			

Until 31th Dec
May go to level 7

Sheet1 / Sheet2 / Sheet3

Sheet 1 / 3   Default   STD   Sum=0   100%

Evolveum

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

*) Identity and Access Management

Manager's View
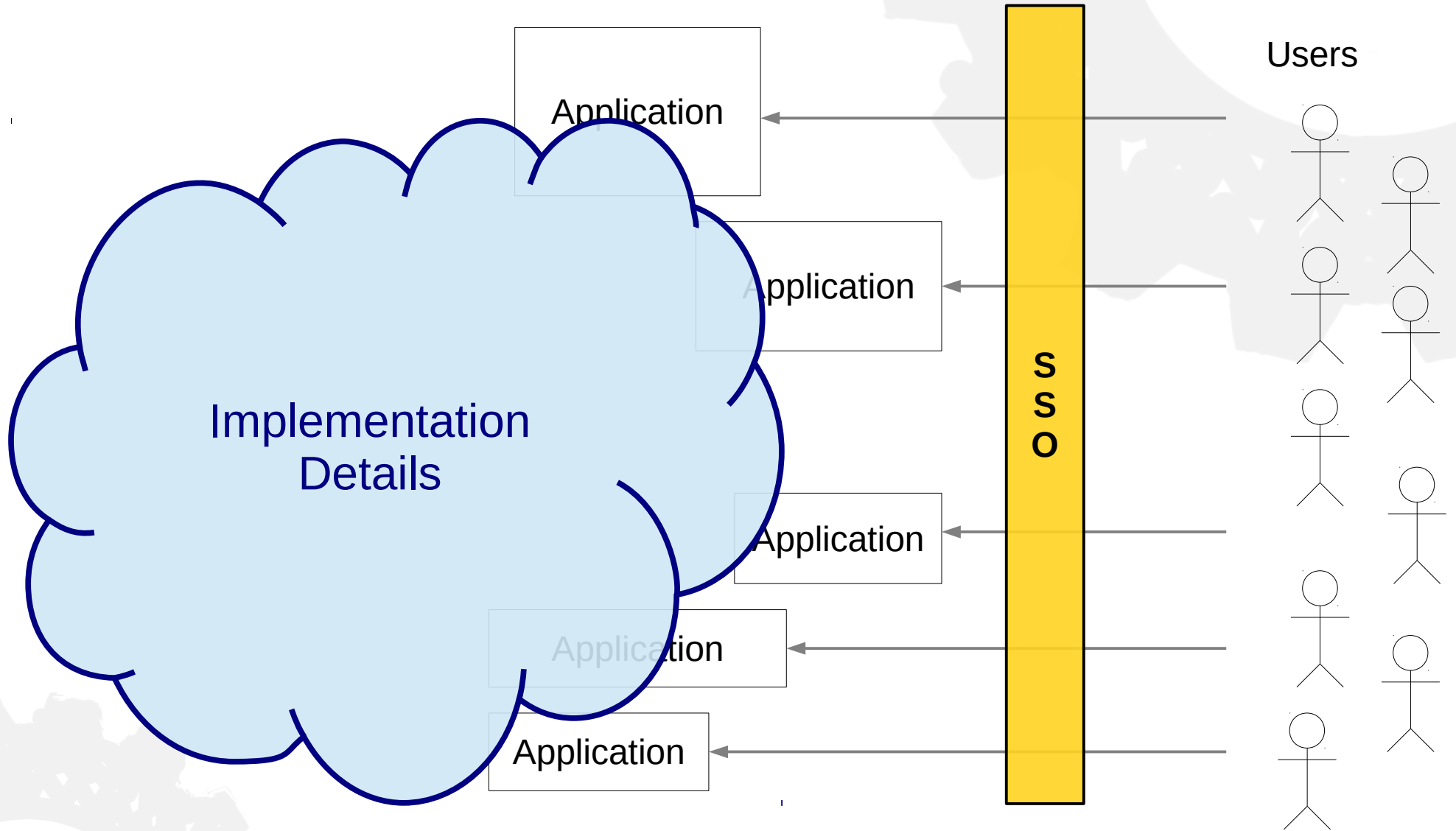
High Level Architect's View

Reality

Relational database

Unsupported

HR

Application

Users

Unsupported

Incompatible identifiers

Application

Local copy

No standard
(ugly script needed)

LDAP

S S O

Custom schema

Application

Incompatible schema

Application

Expensive

Application

Home directory

Extremely expensive

Evolveum
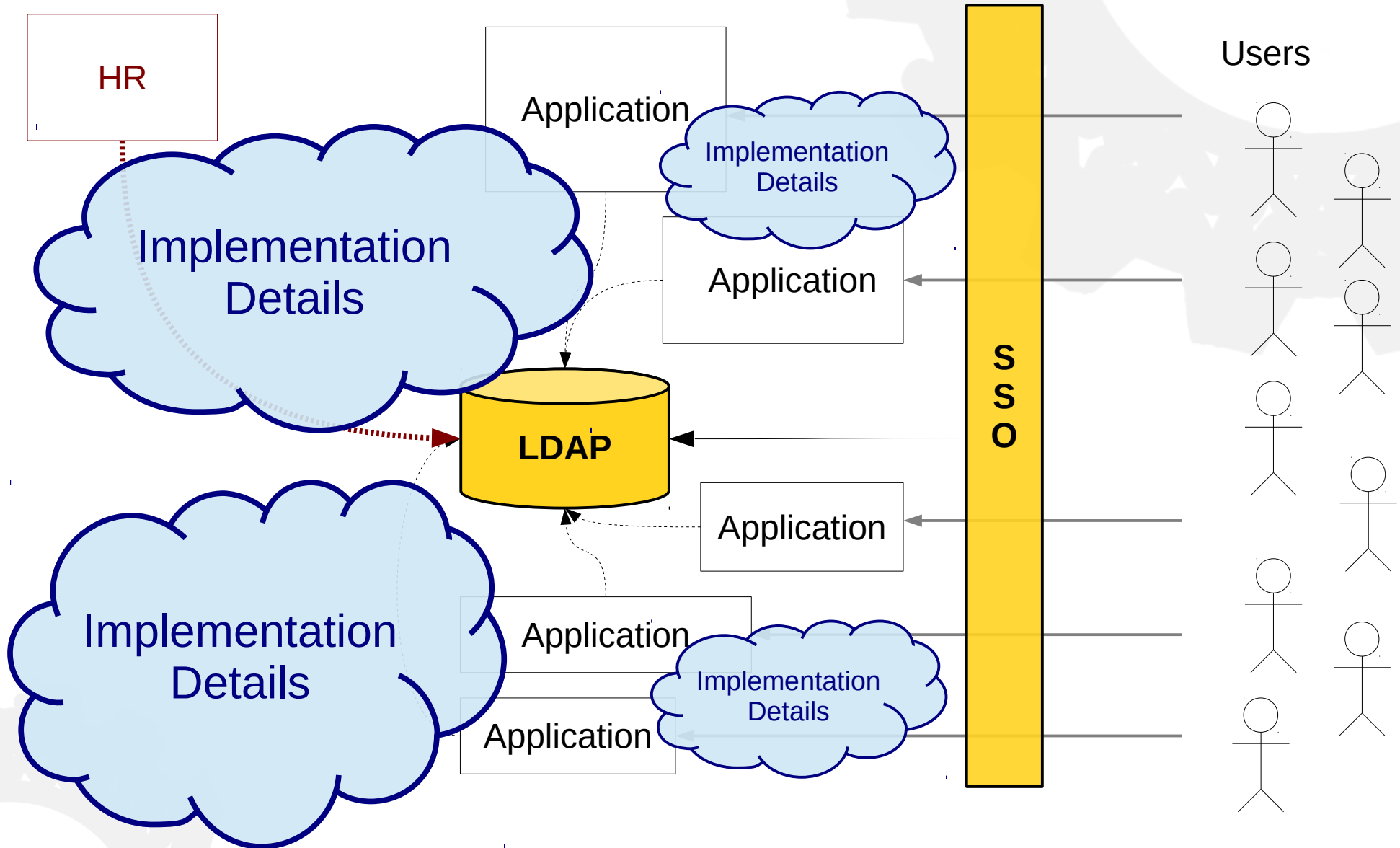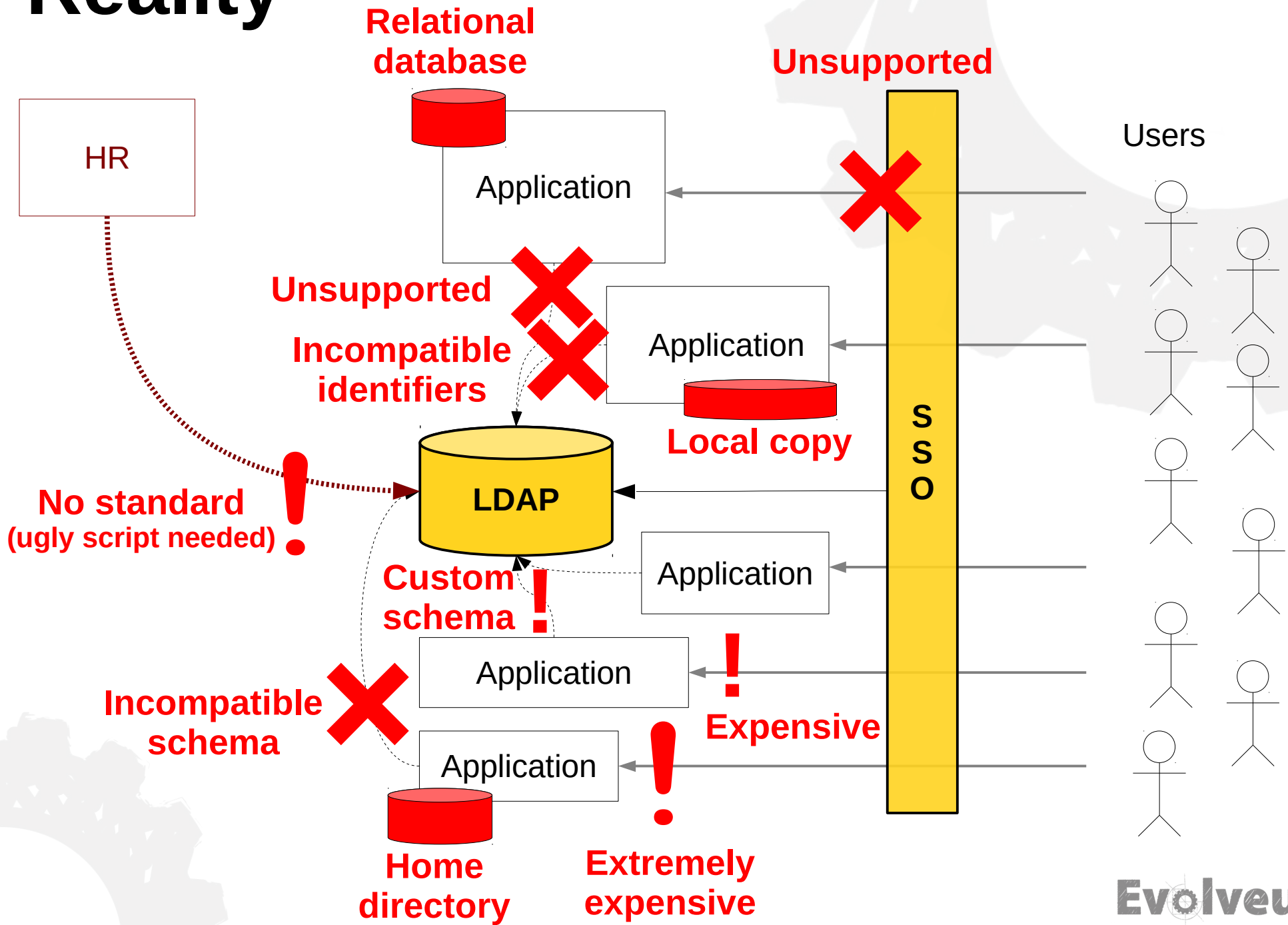
"Single directory" approach is not going to work

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

Evolveum

What are we going to do now?

DO NOT PANIC!
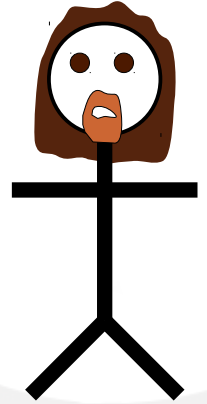
SSO is what you think you **want**

IDM is what you really **need**

Evolveum

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

Evolveum

Identity and Access Management

System Admin

Requester Approver

Application

Users

Identity Management

Application

Identity Repository

HR

Application

A M

Application

CRM

Application

Evolveum

How IDM works?

Identity Management

Application

Application

Identity Repository

HR

A M

Application

Application

Evolveum
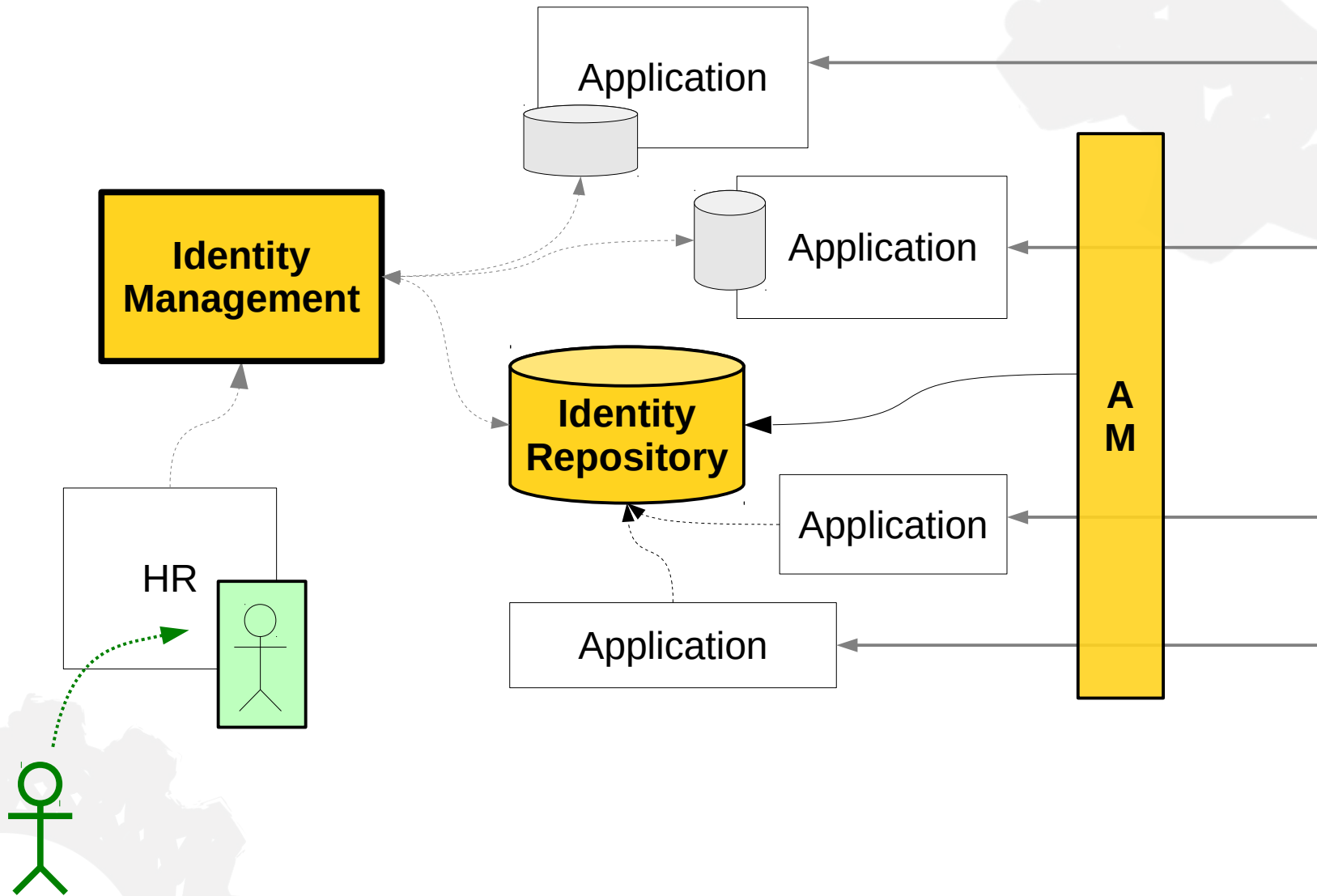
Automatic user provisioning

Policies
RBAC
Rules

Identity Management

HR

Identity Repository

Application

Application

Application

Application

AM
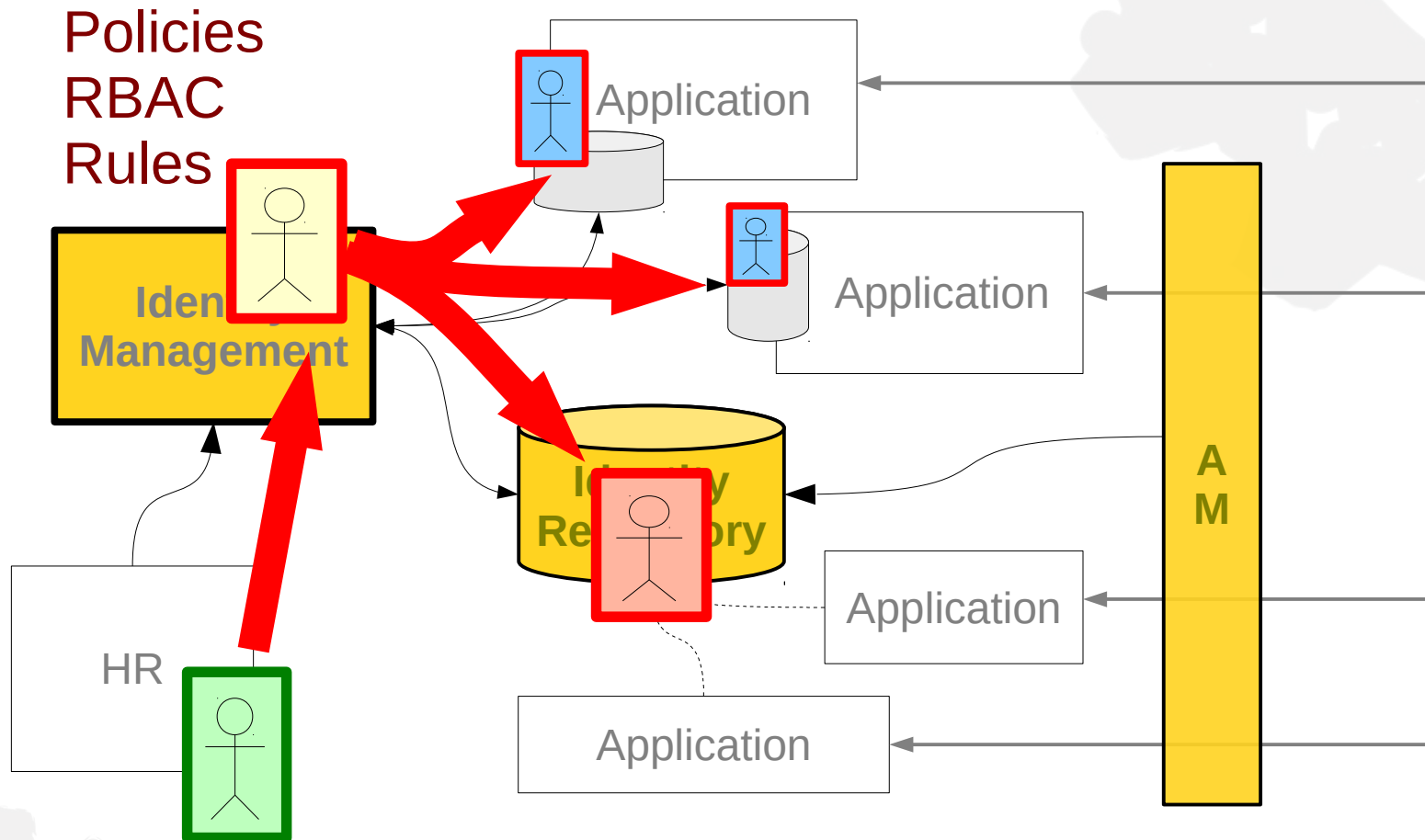
Business As Usual

Password reset (self-service)
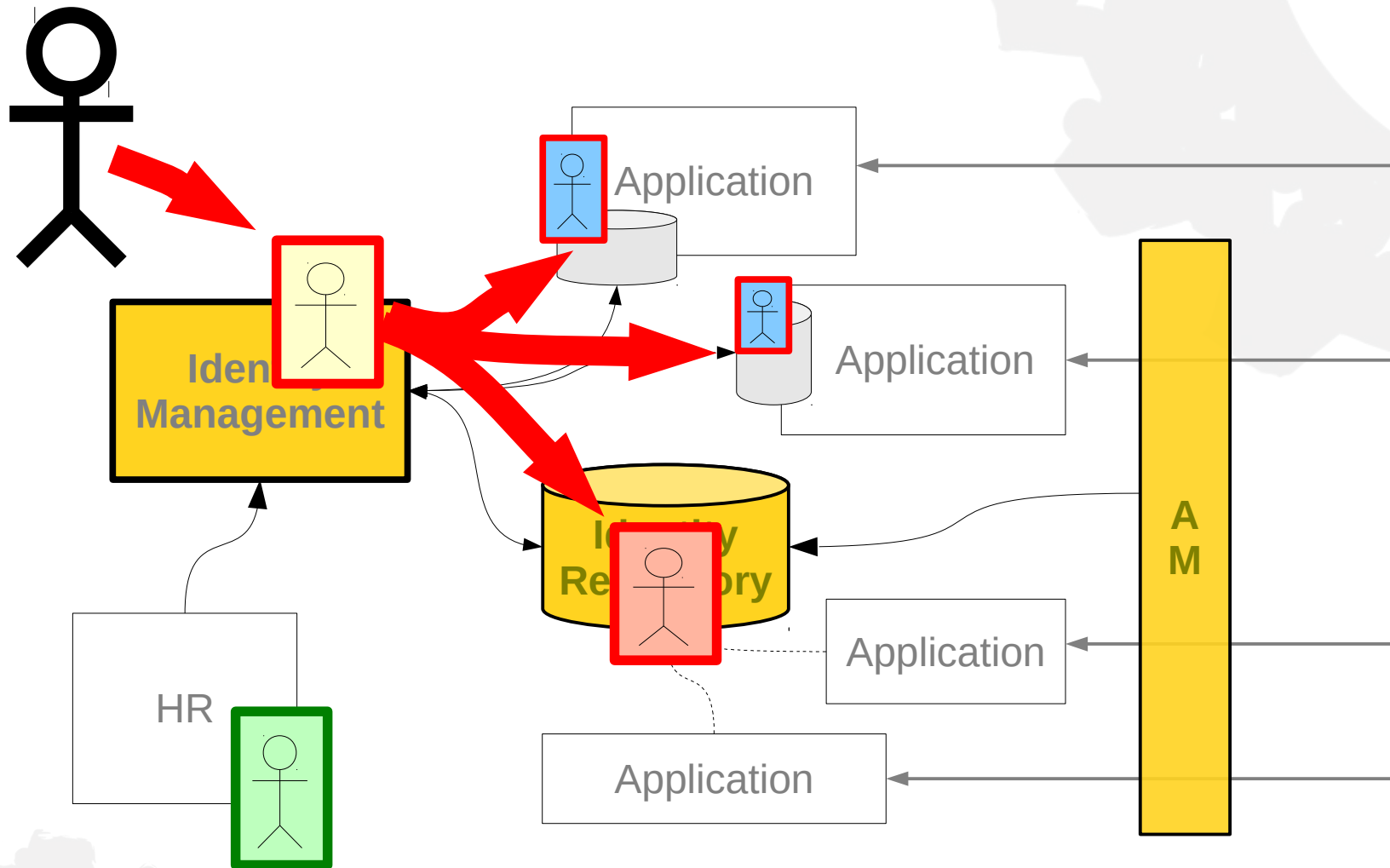
Employee Leaves Company
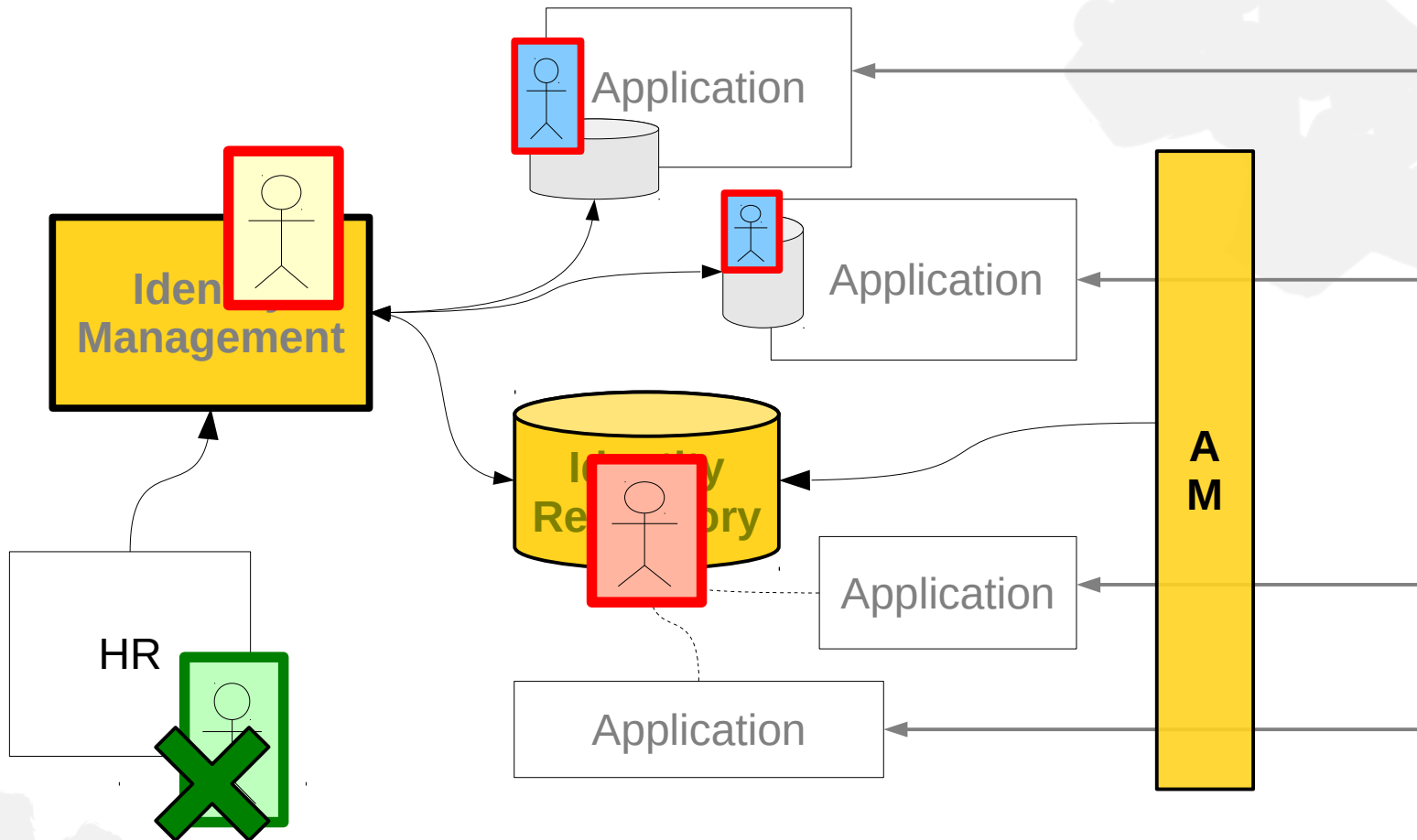
Automatic user deprovisioning

Business As Usual

Identity Management

HR

Application

Application

Identity Repository

Application

Application

A M

Evolveum
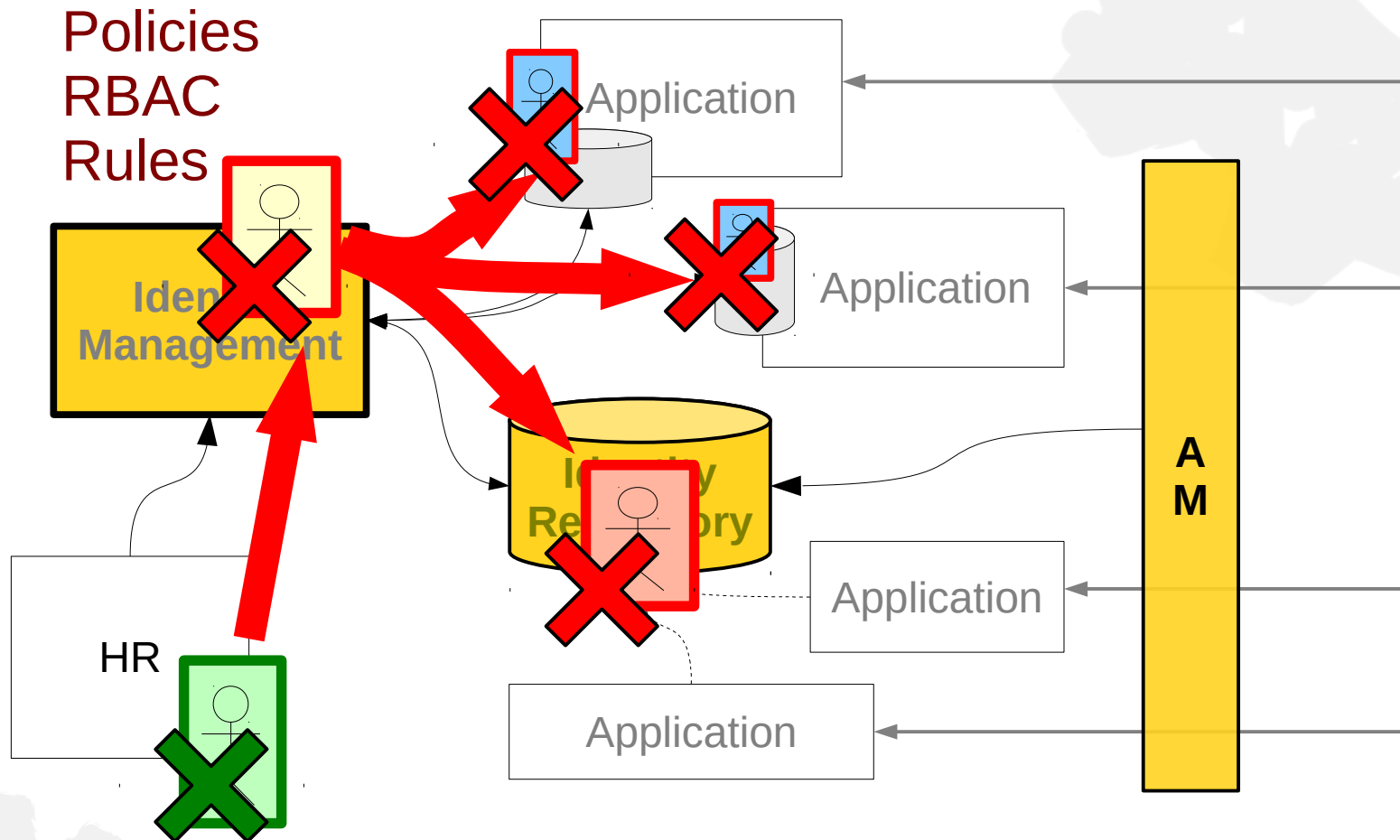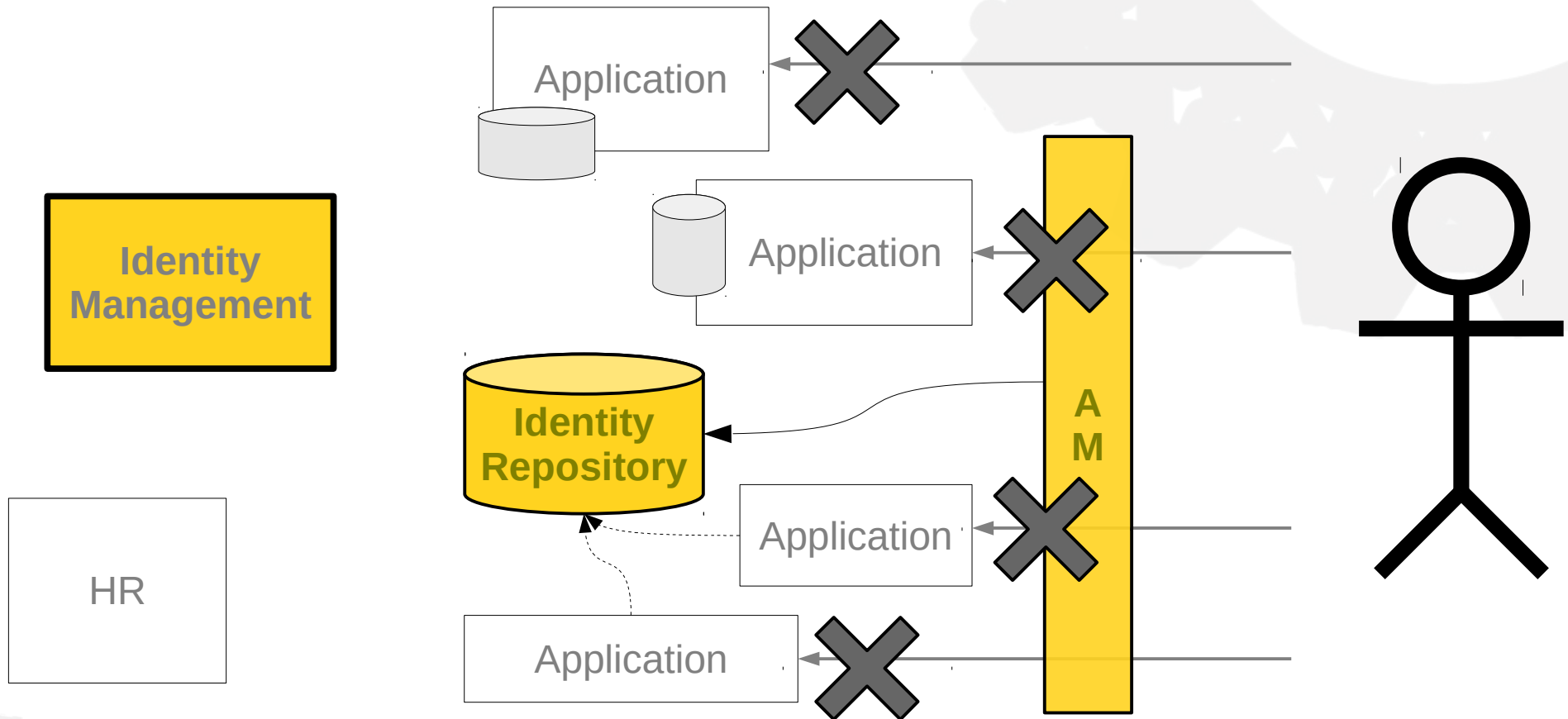
Bidirectional Synchronization

Policy enforcement

Policies
RBAC
Rules

Identity Management

HR

Application

Application

Identity Repository

Application

Application

A M

Evolveum
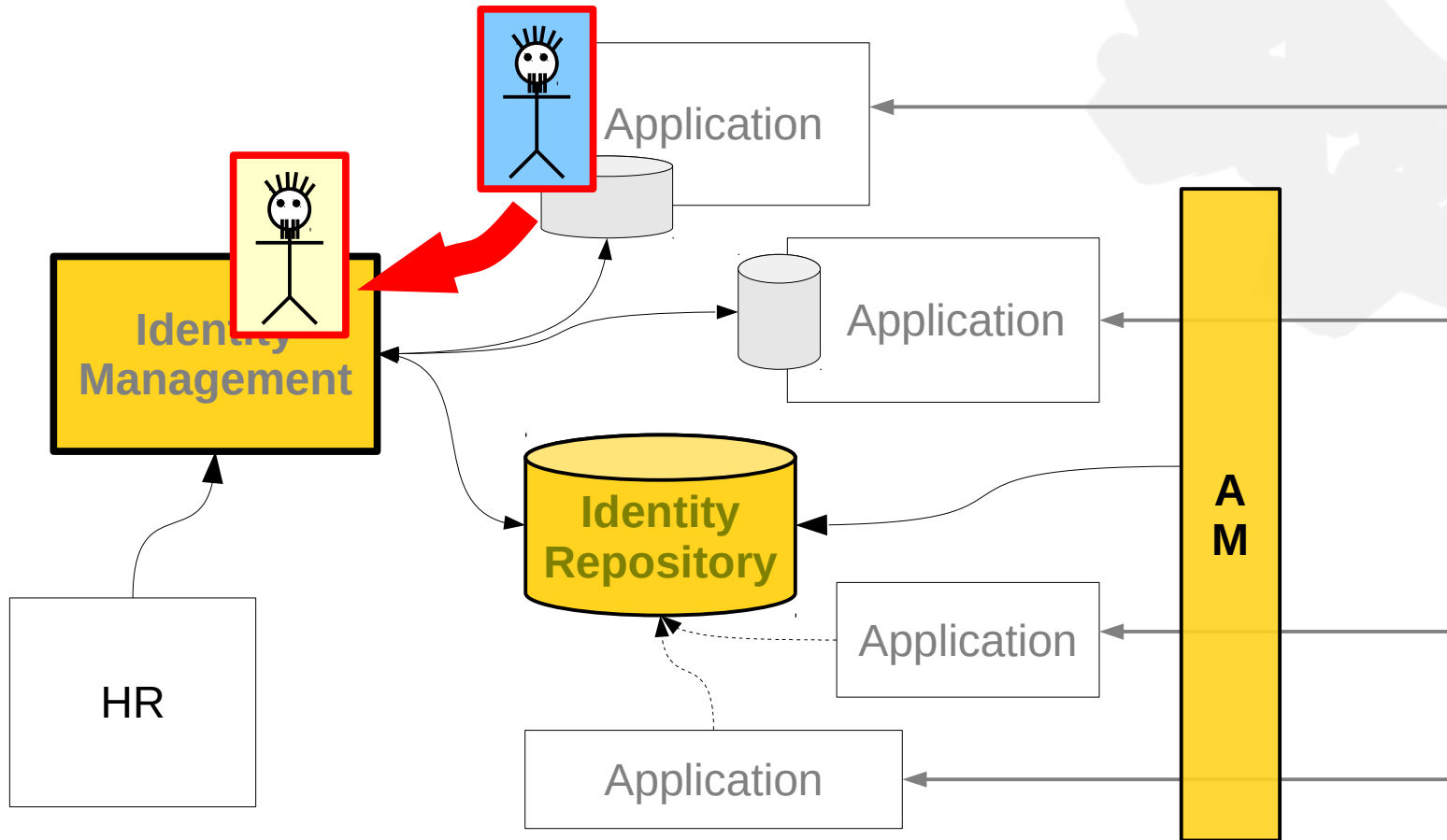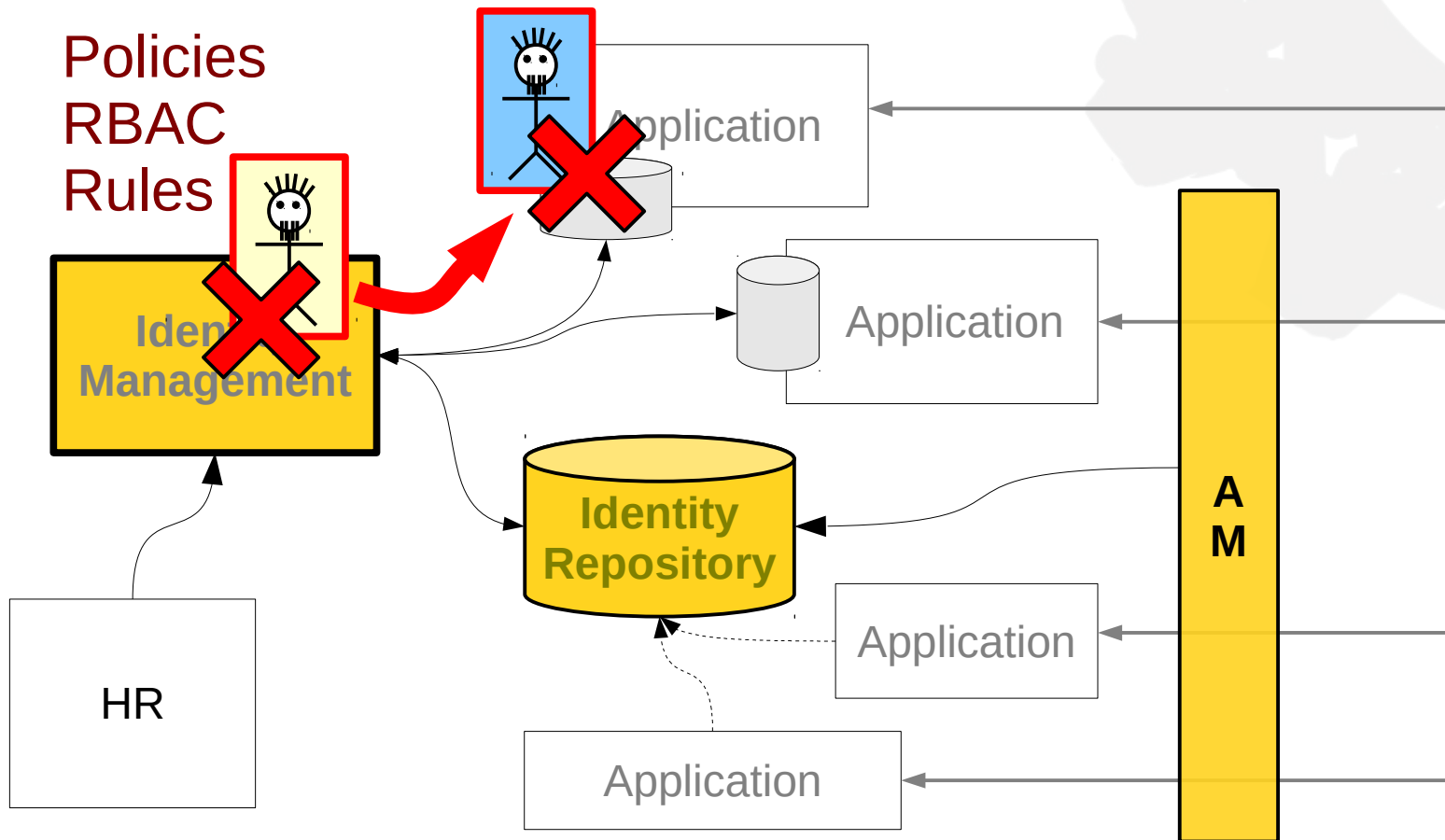
What Identity Management does?

- 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

- ...

Evolveum

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!

Evolveum

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

Evolveum

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.

Evolveum

Open Source to the Rescue

There was no practical FOSS solution until 2010

       (Sun Identity Manager was the king)

2010-2011: Syncope, OpenIDM, midPoint, ...
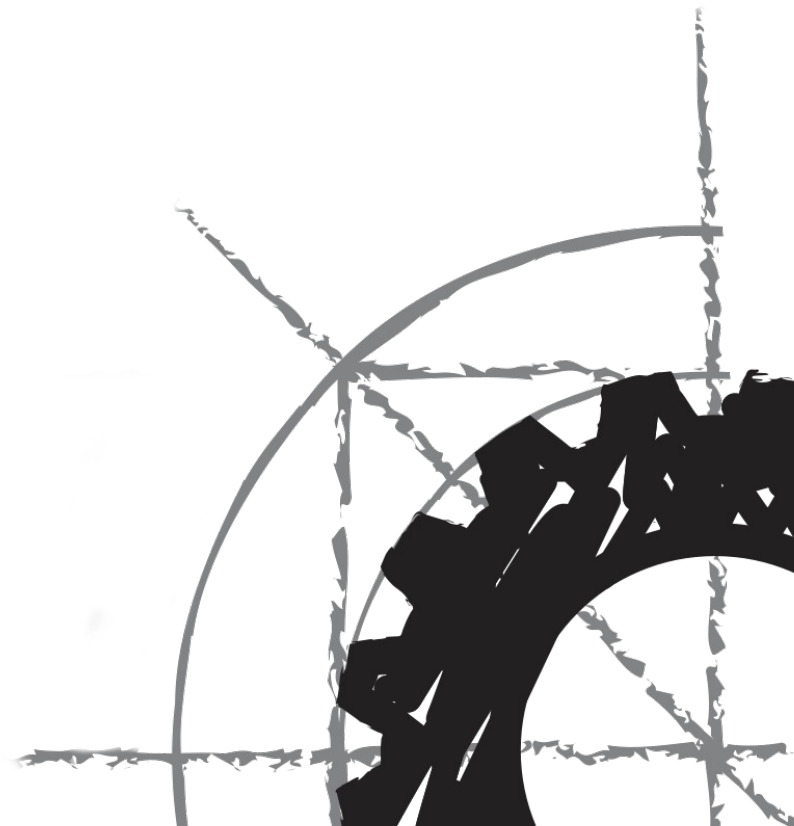
       (that was the time when Oracle acquired Sun)

Now there are two leading open source[*] IDMs:

- Apache Syncope

- Evolveum midPoint

*) by "open source" I mean both license and practice

Evolveum

Evolveum midPoint?

Evolveum
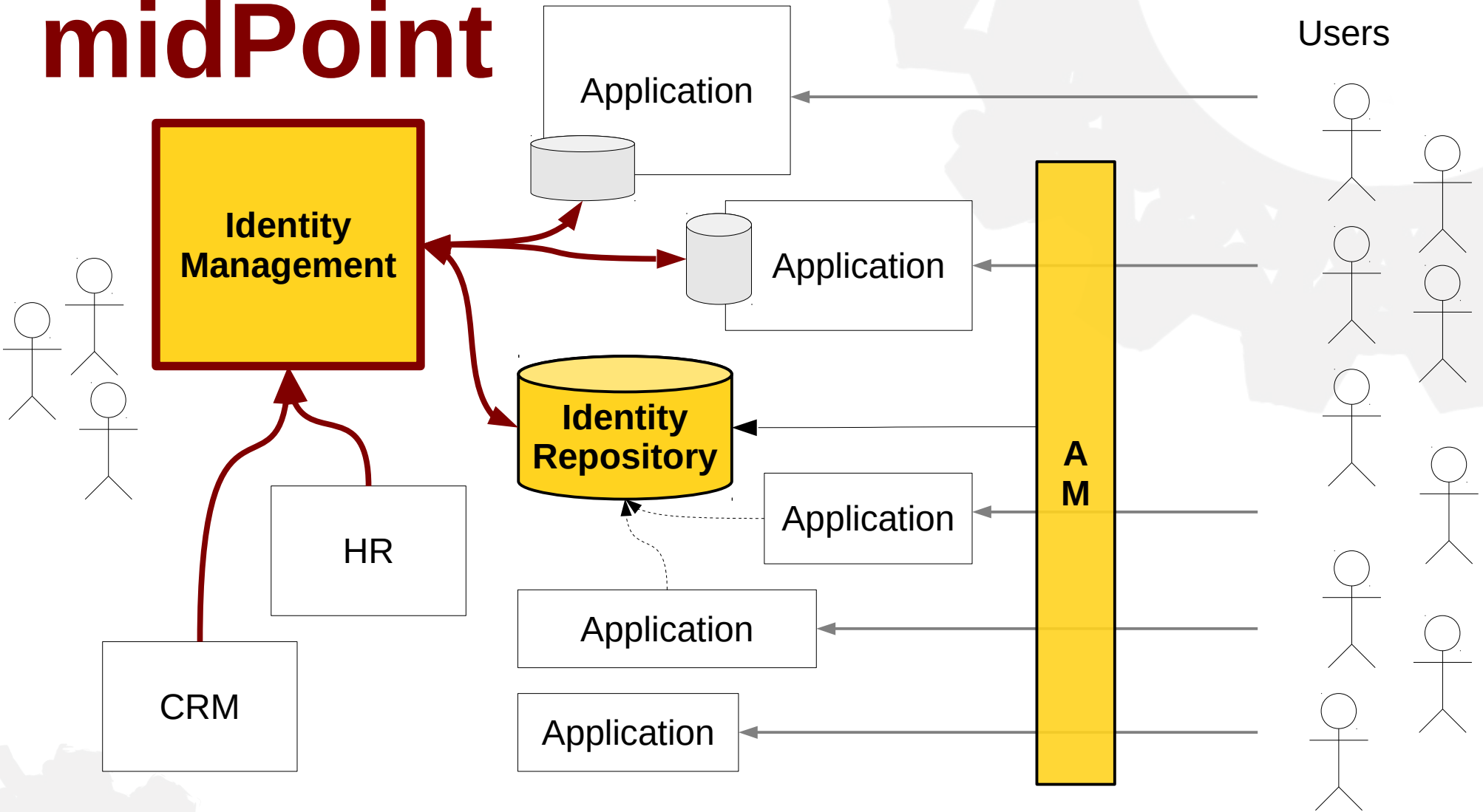
The midPoint Story

- 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 Authorization Localization Notifications

Scripting Self-service Audit Data mapping REST Identifiers

Parametric roles Delegated administration

Bulk actions

Evolveum

MidPoint Big Picture

Target Systems

midPoint

Source Systems

Identity Connectors
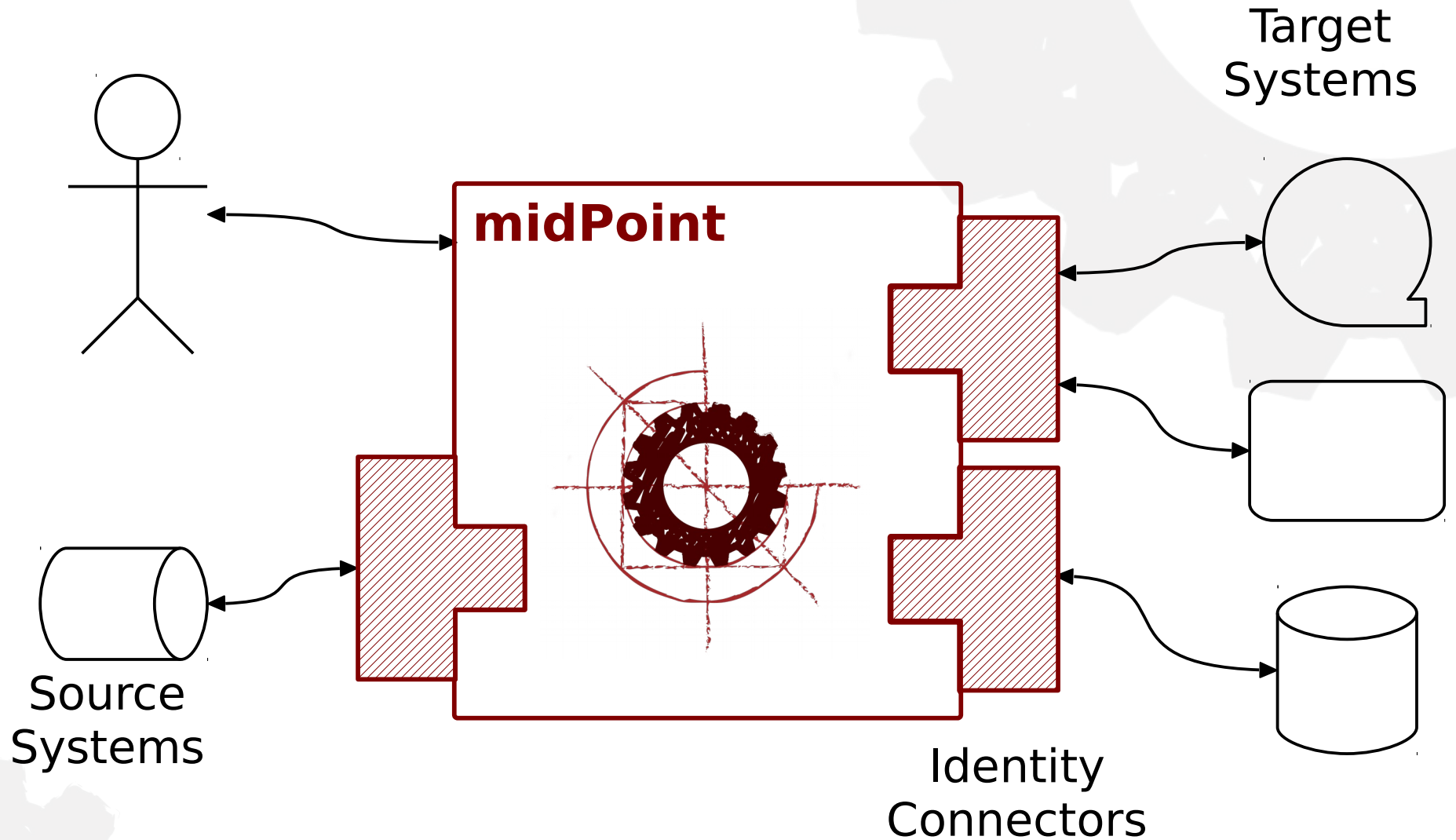
Evolveum

Complete Open Source Solution

midPoint
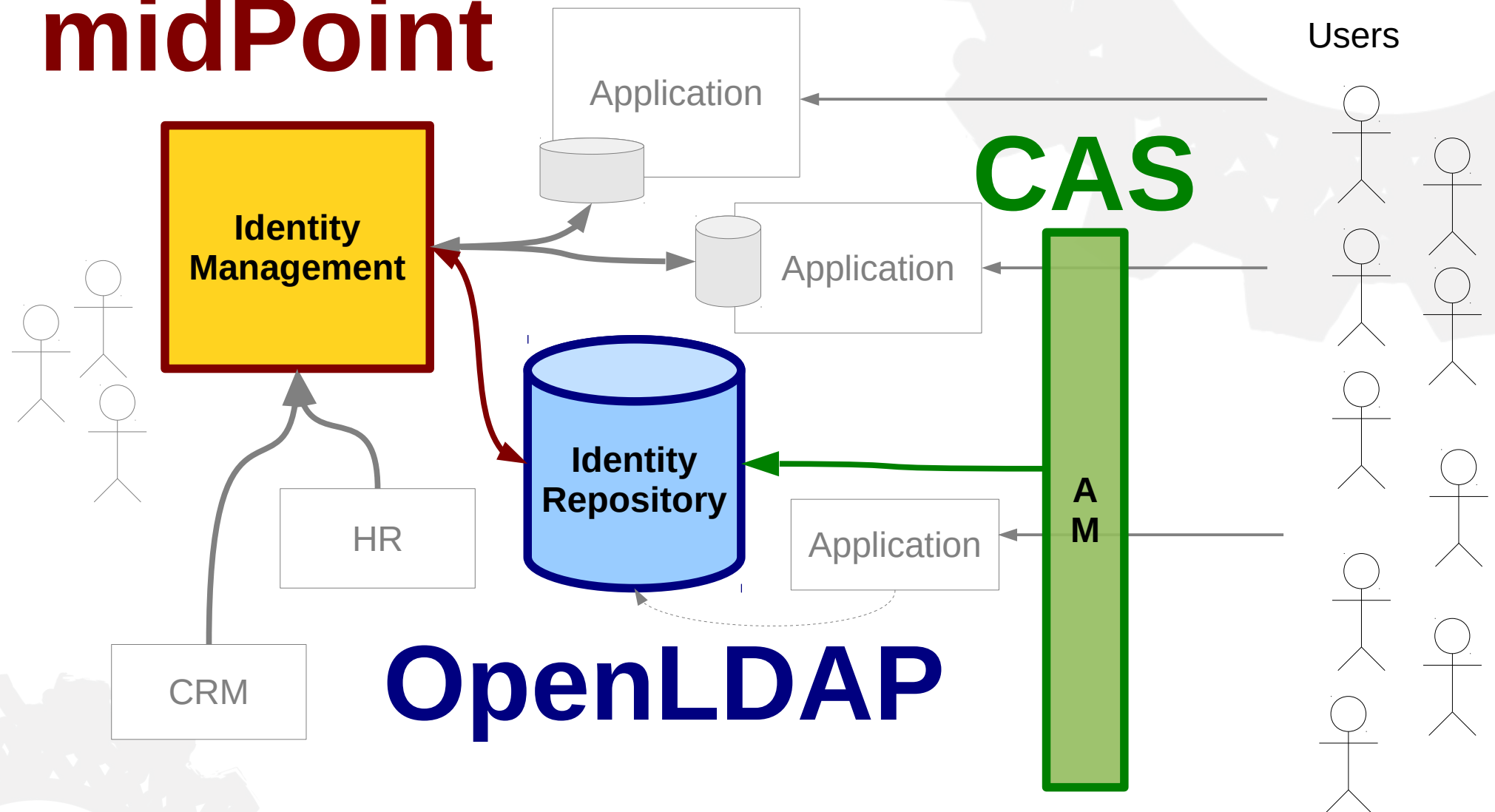
CAS
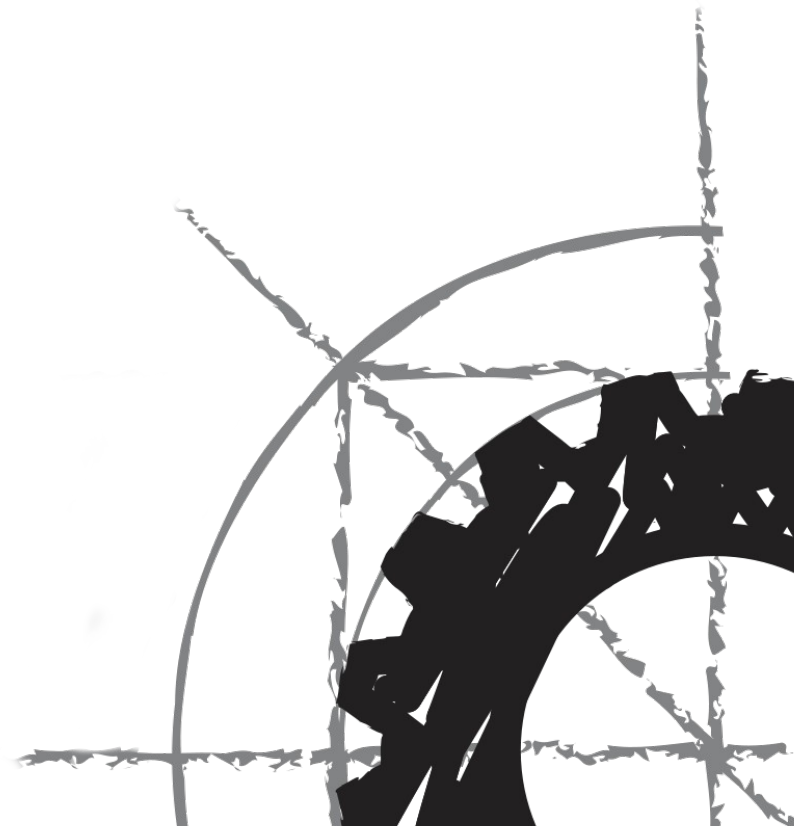
Users

Application

Identity Management

Application

Identity Repository

A M

HR

Application

OpenLDAP

CRM

Evolveum

Conclusion

Identity and Access Management

IAM Letter Soup

IDM

- System Admin
- Requester
- Approver
- Connector
- Administration
- Policy
- RBAC
- Workflow
- Provisioning
- LDAP
- Sync
- AD
- Integration

AM

- Authentication
- SSO
- LDAP
- Two-factor
- OAuth
- OpenID Connect
- Federation
- UMA
- SAML

Users

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
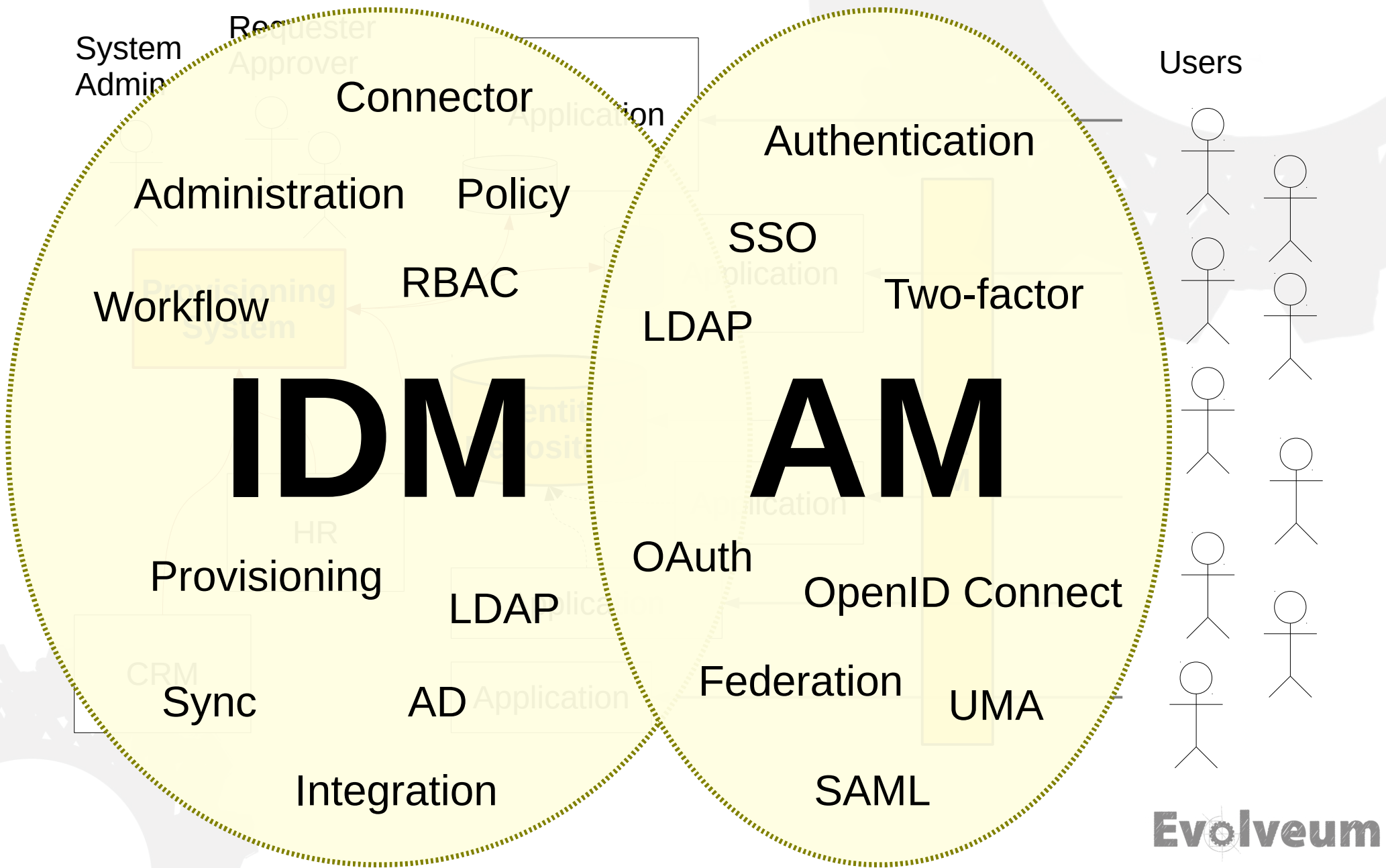
Evolveum

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

START HERE

Evolveum

Questions and Answers

Conditions Expressions Provisioning Management Schema Extensibility

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

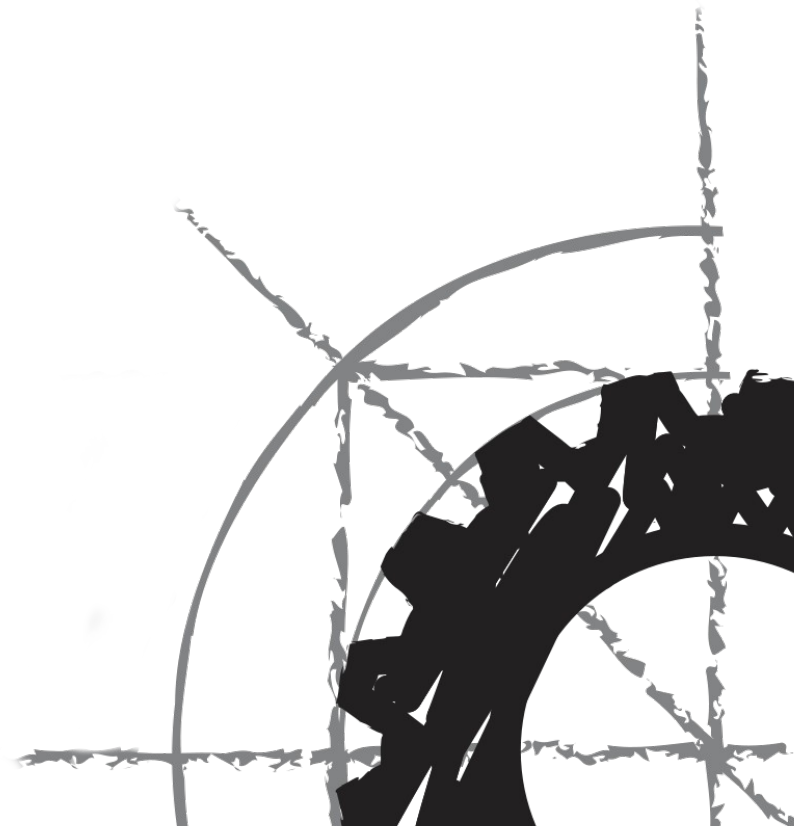Parametric roles Delegated administration

Bulk actions

Evolveum

Thank You
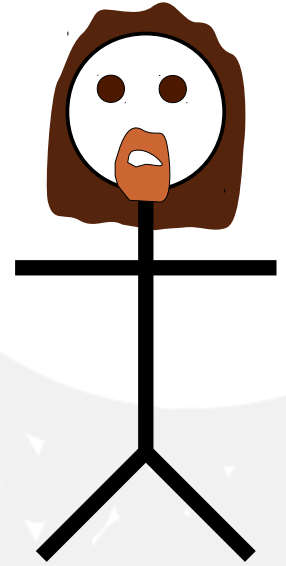
Radovan Semančík

www.evolveum.com

Evolveum

Extra Slides

(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

Evolveum

Example midPoint Deployment Architecture
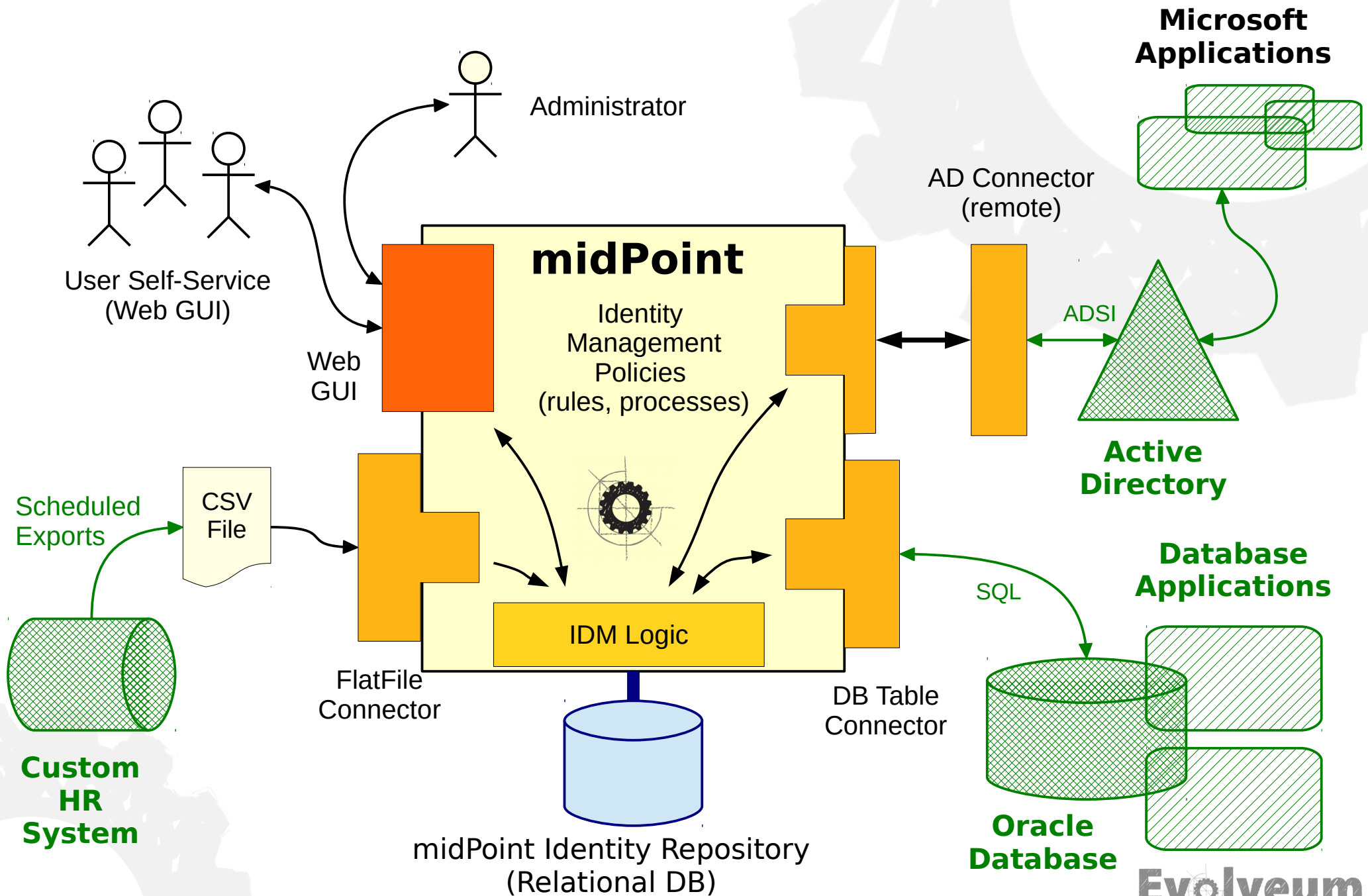
Identity Connectors

- ## 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

Evolveum

Live Demo

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

Documentation: search for "Live demo" in wiki.evolveum.com

Evolveum