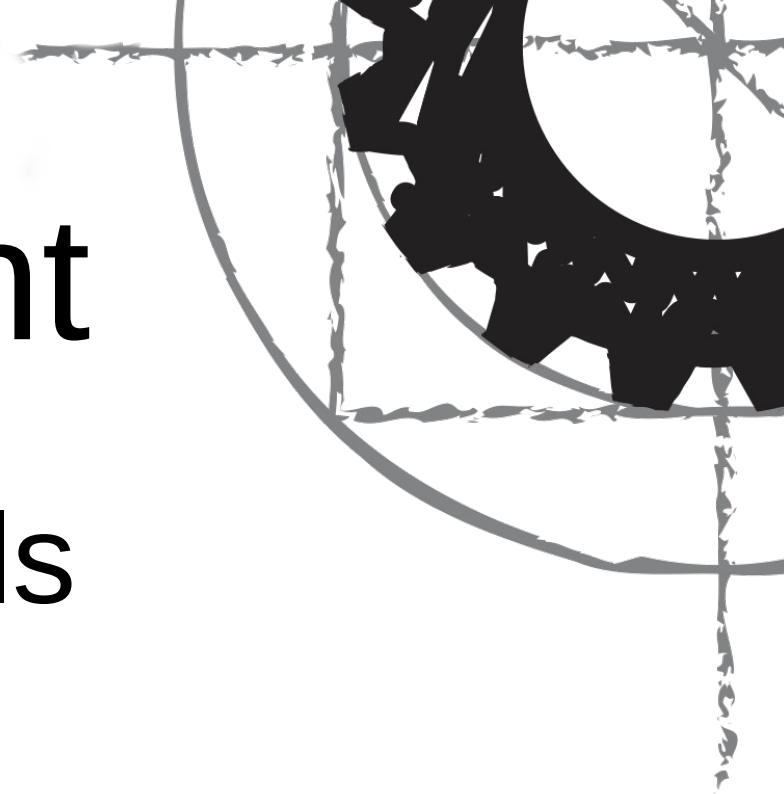


Project midPoint or how a handful of fools fought the Giants



Radovan Semančík
Open Source Weekend, April 2016

Radovan Semančík



Current:

Software Architect at **Evolveum**

Architect of Evolveum **midPoint**

Contributor to **ConnId** and **Apache Directory API**

Past:

Sun LDAP and IDM deployments (early 2000s)

OpenIDM v1, OpenICF

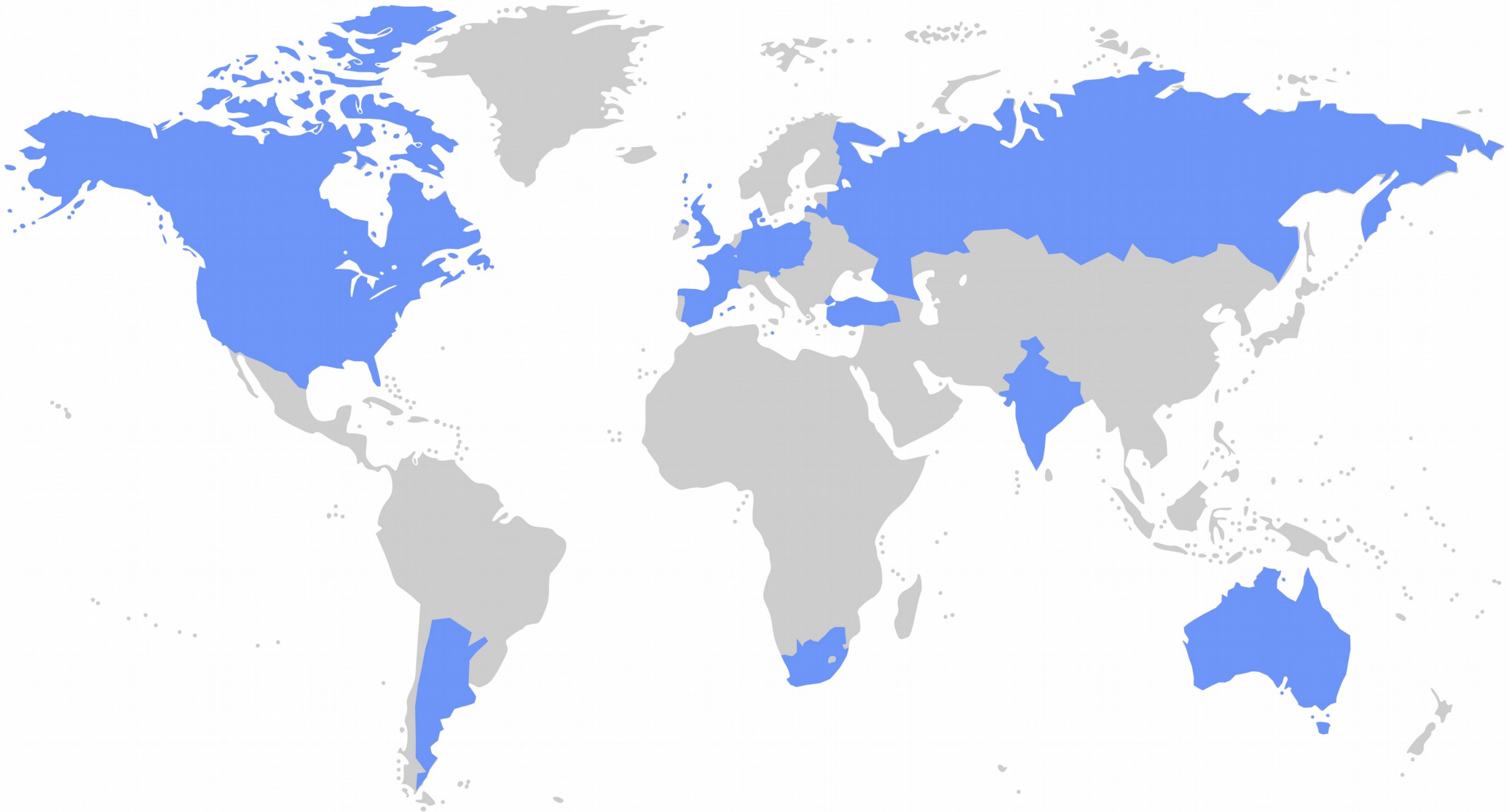
Many software architecture and security projects

Project midPoint

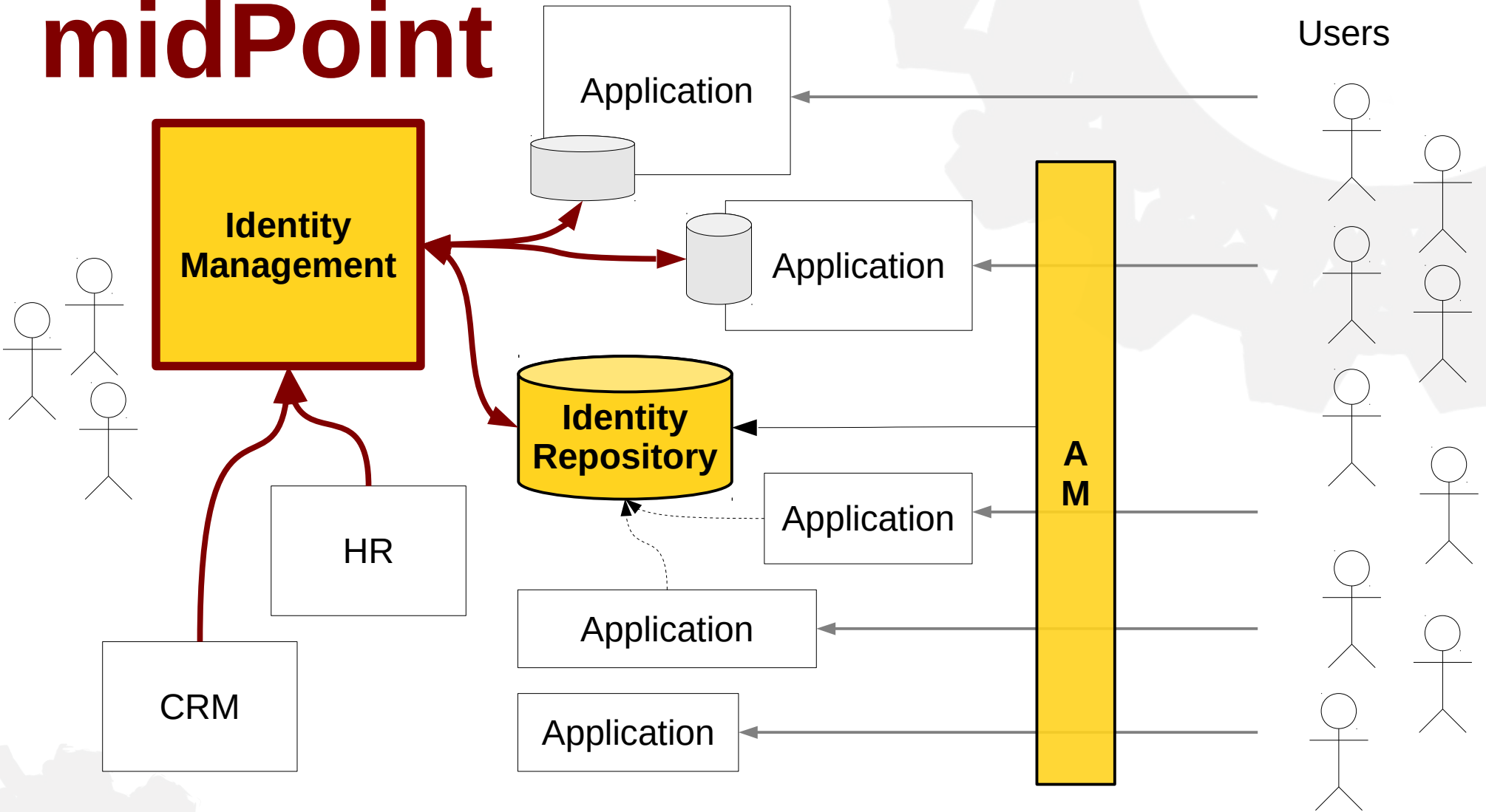
- Advanced **Identity Management** Product
- Started 2010-2011 (**5+ years**, 16 releases)
- more than **500K lines of code** (Java)
- **World-wide** recognition

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

midPoint is used all around the world



midPoint





There is **no security** without
identity management

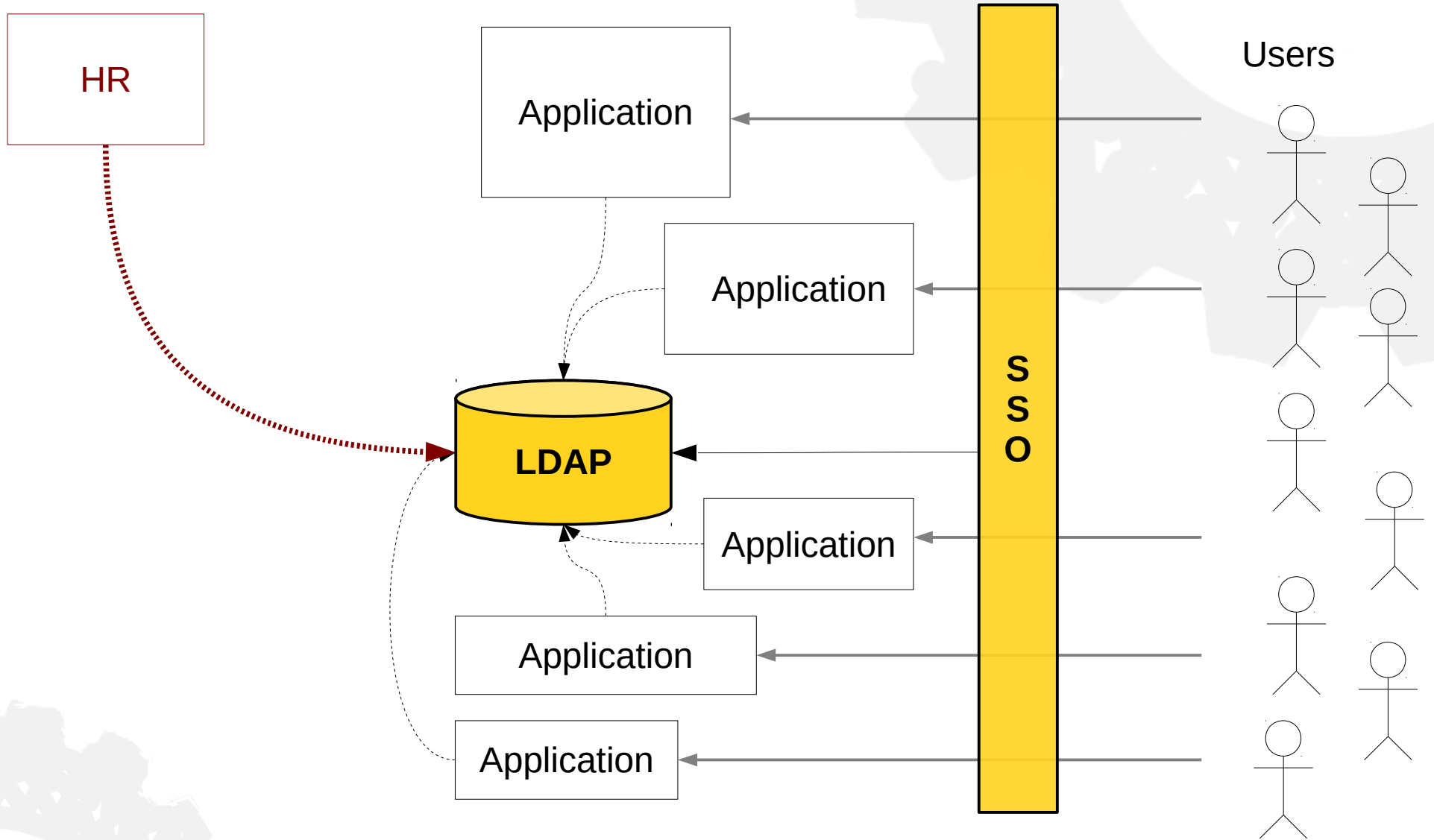
If you have no IDM, how can you be sure that ...

- illegal accounts are disabled/deleted?
- temporary accounts are deleted?
- users have only the least privileges?
- the privileges are not accumulated?
- no secondary authentication is possible?
- the data are up to date? (title, affiliation, ...)
- notifications and tasks are suspended?

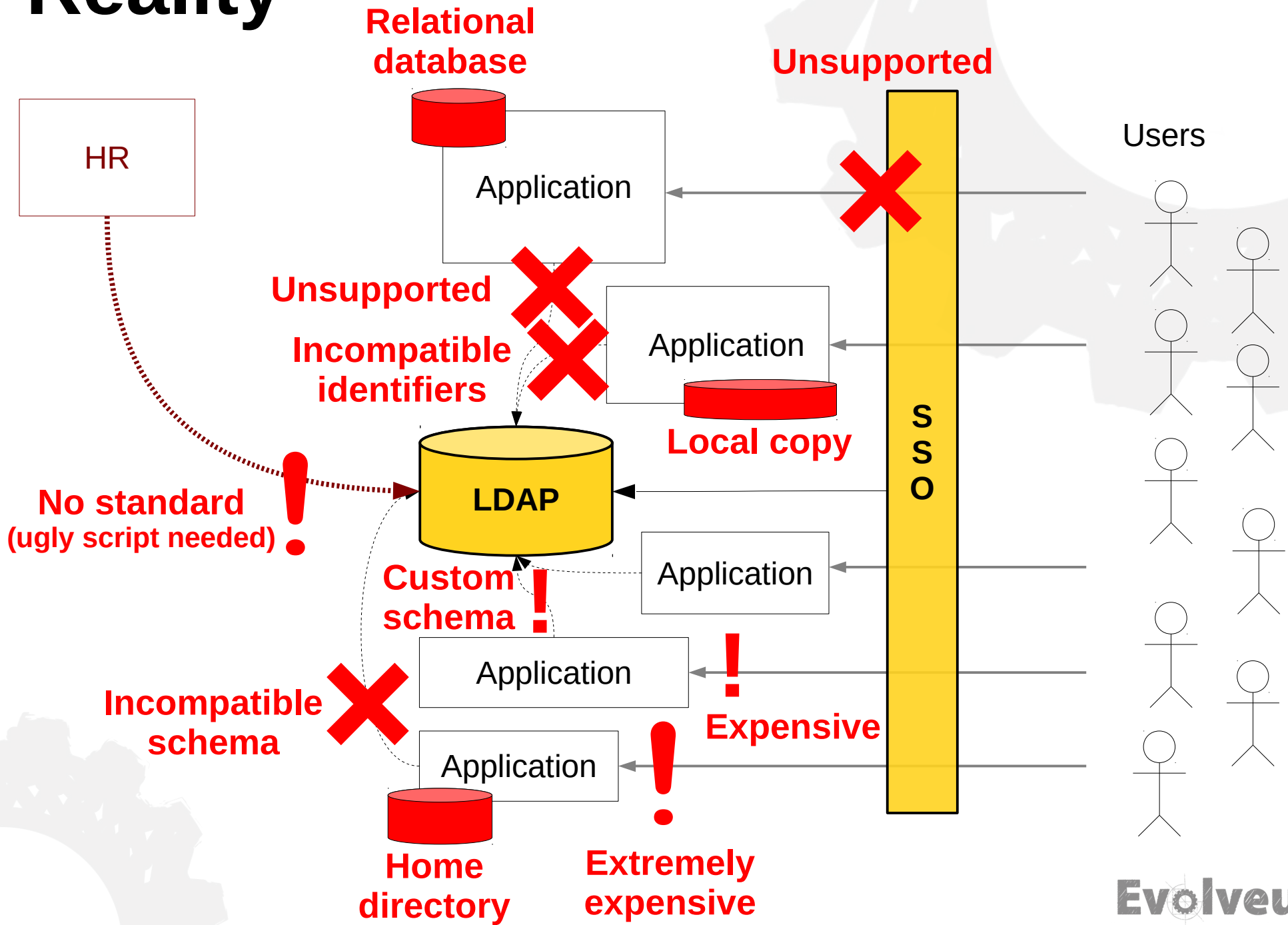


The solution is trivial
Let's put everything in LDAP!

Expectation



Reality





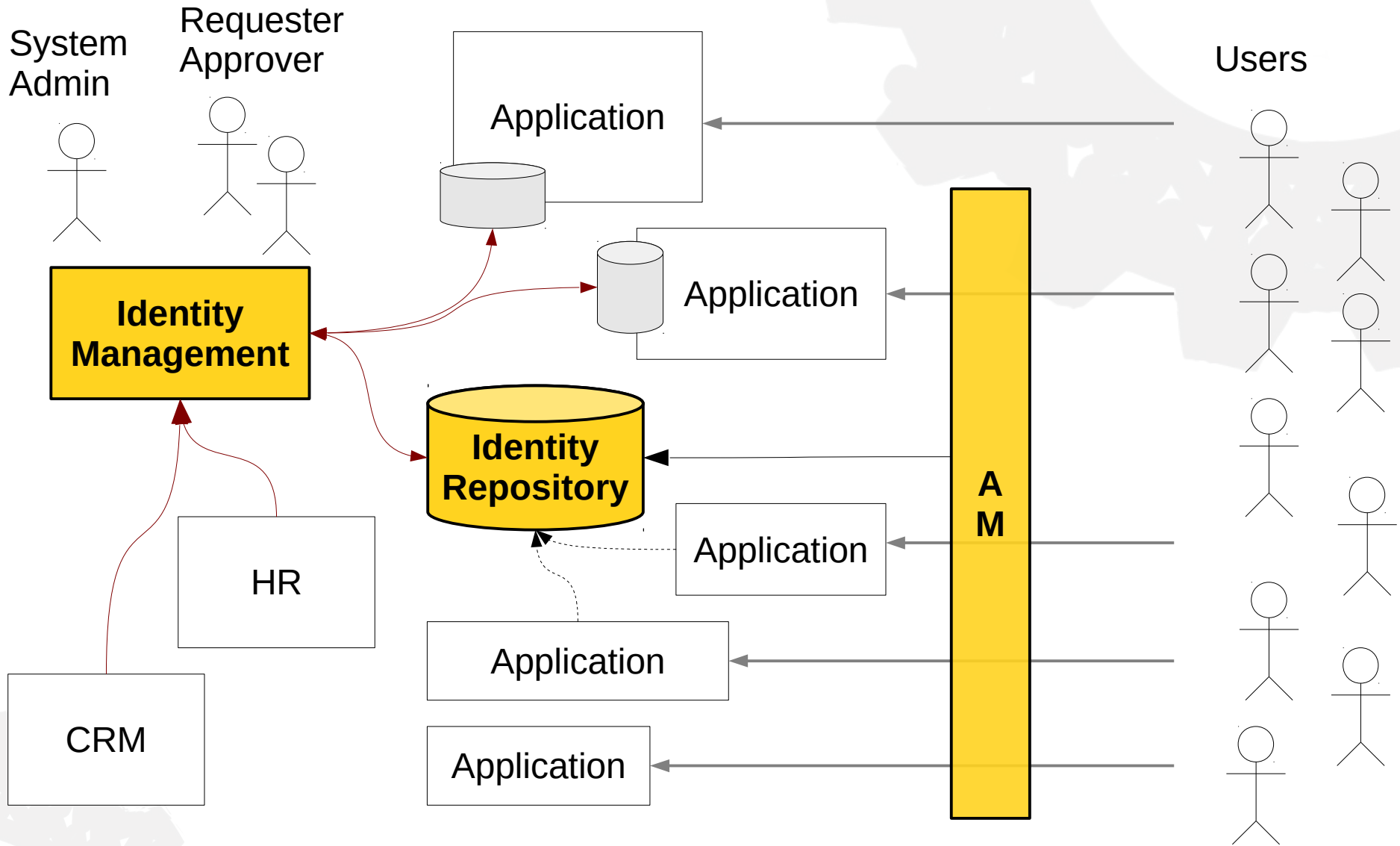
“Single directory” approach is **not going to work**

... and this has been known for 10 years (at least)

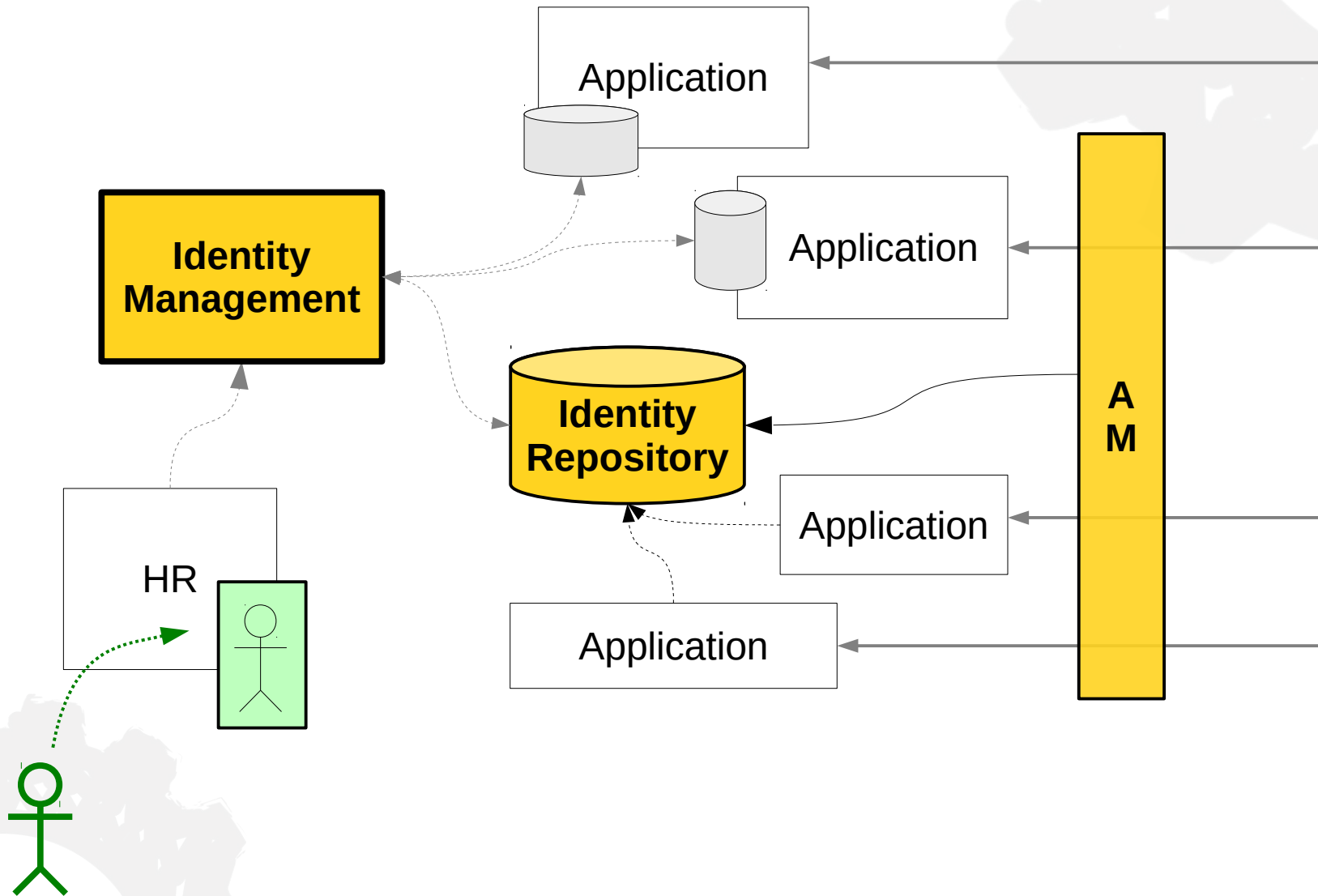


*) yet, it might work well for simple and quite homogeneous environments

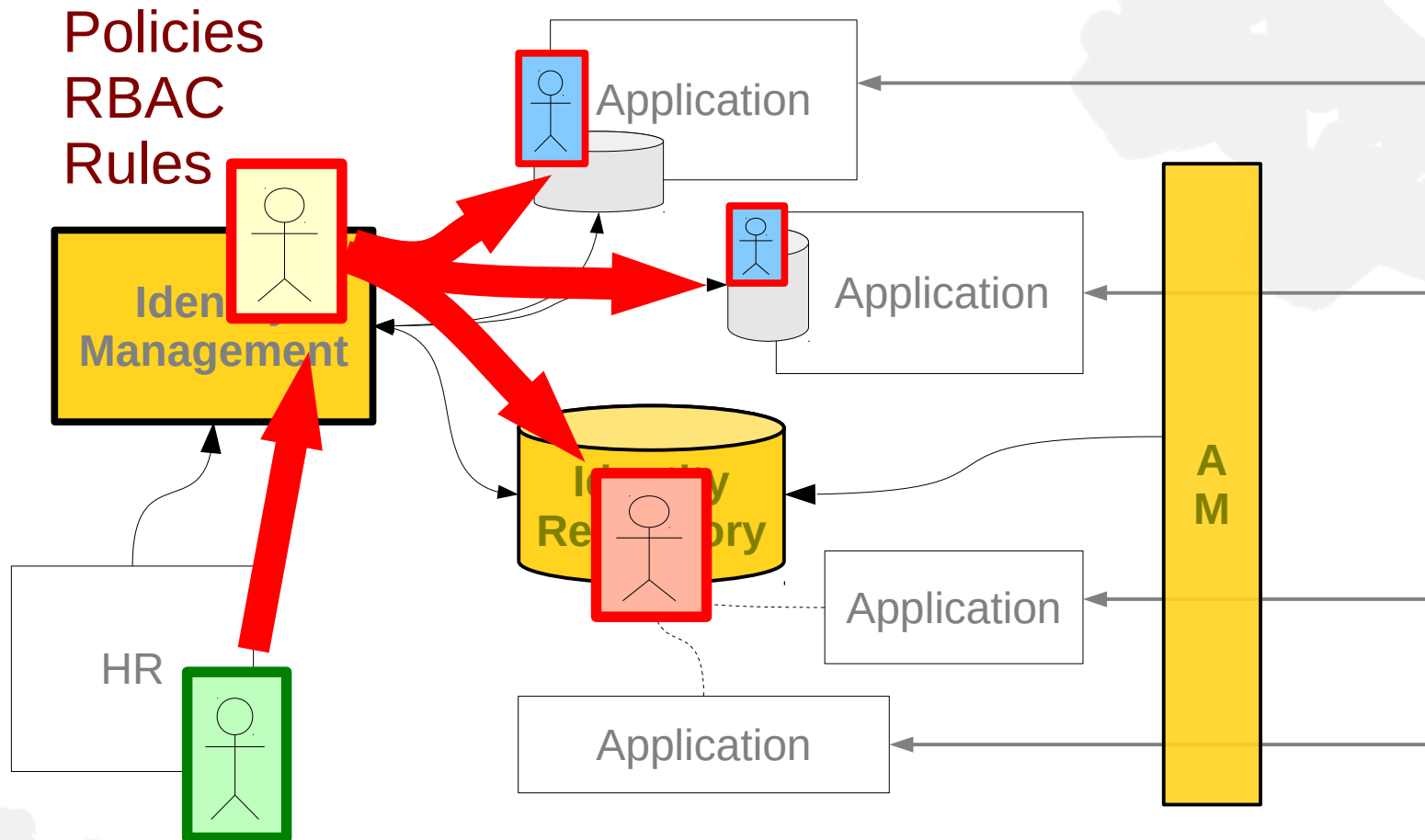
Identity and Access Management



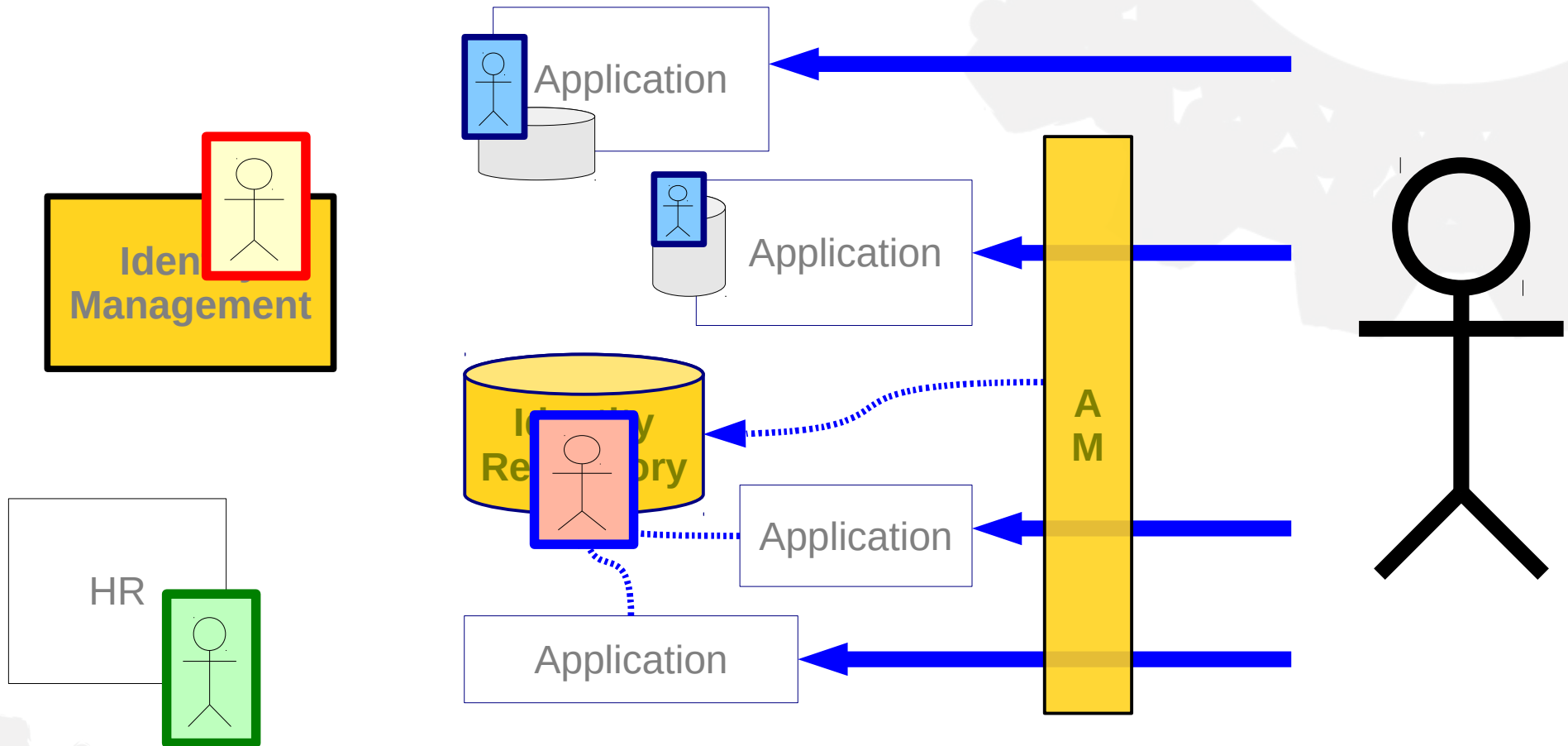
How IDM works?



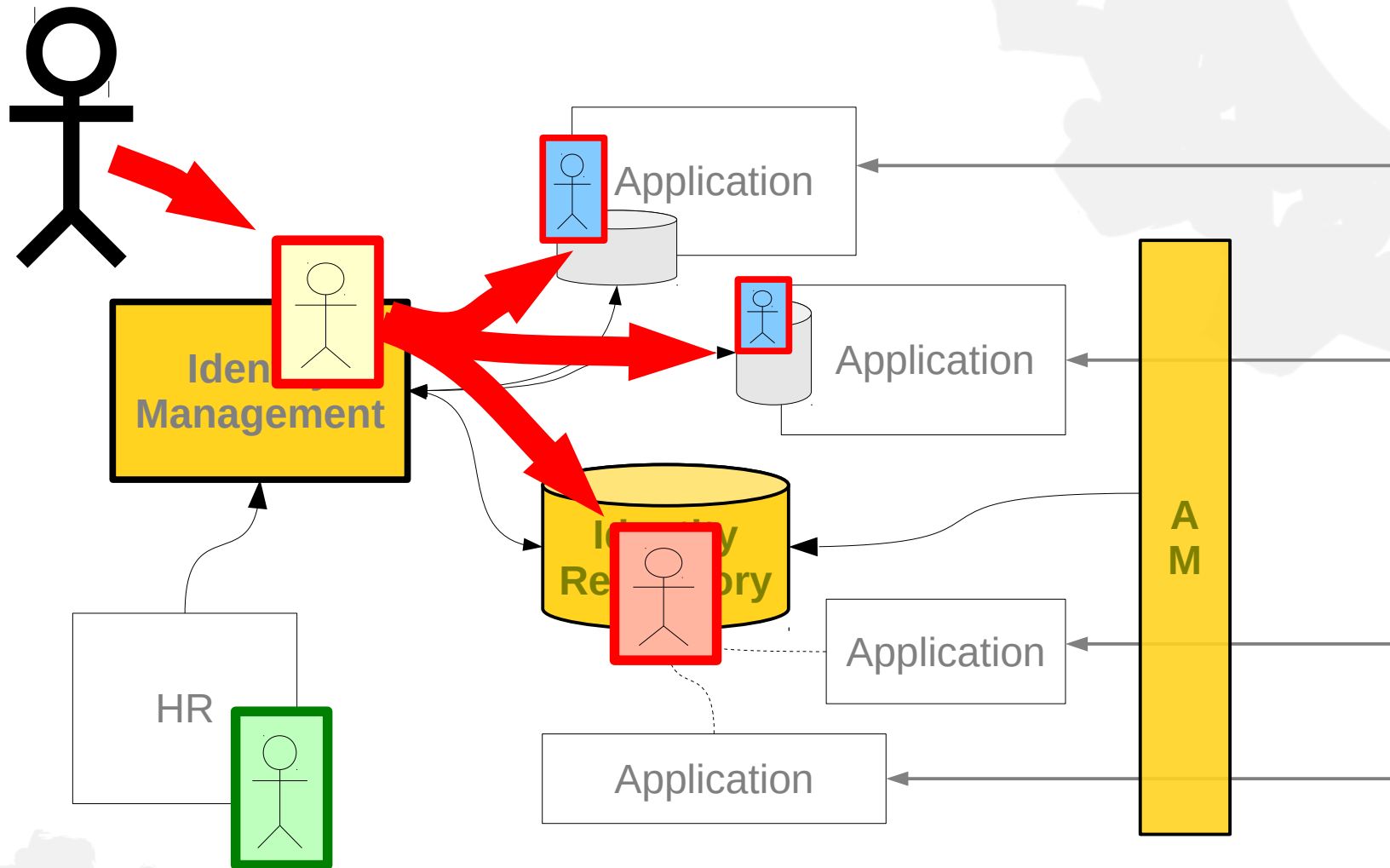
Automatic user provisioning



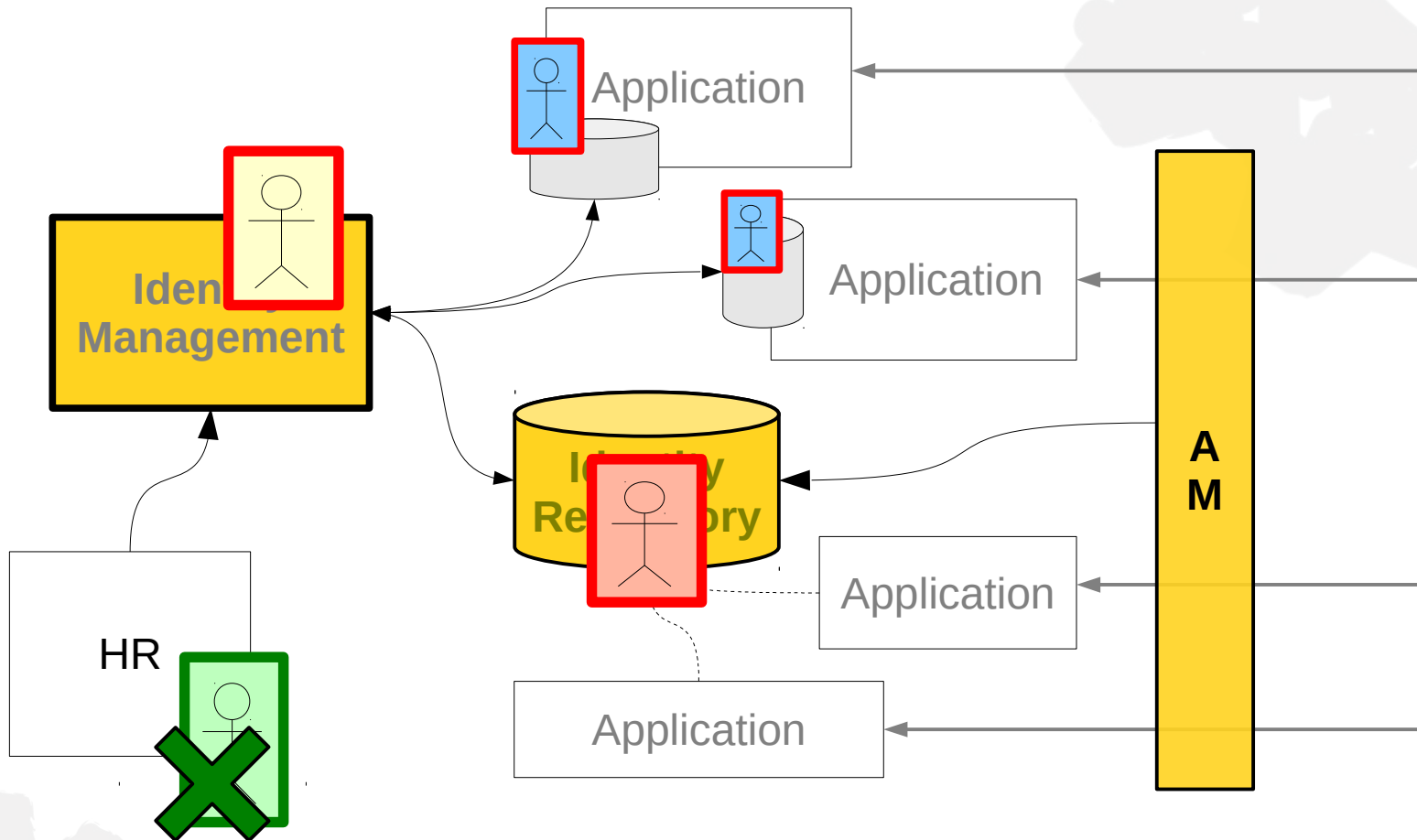
Business As Usual



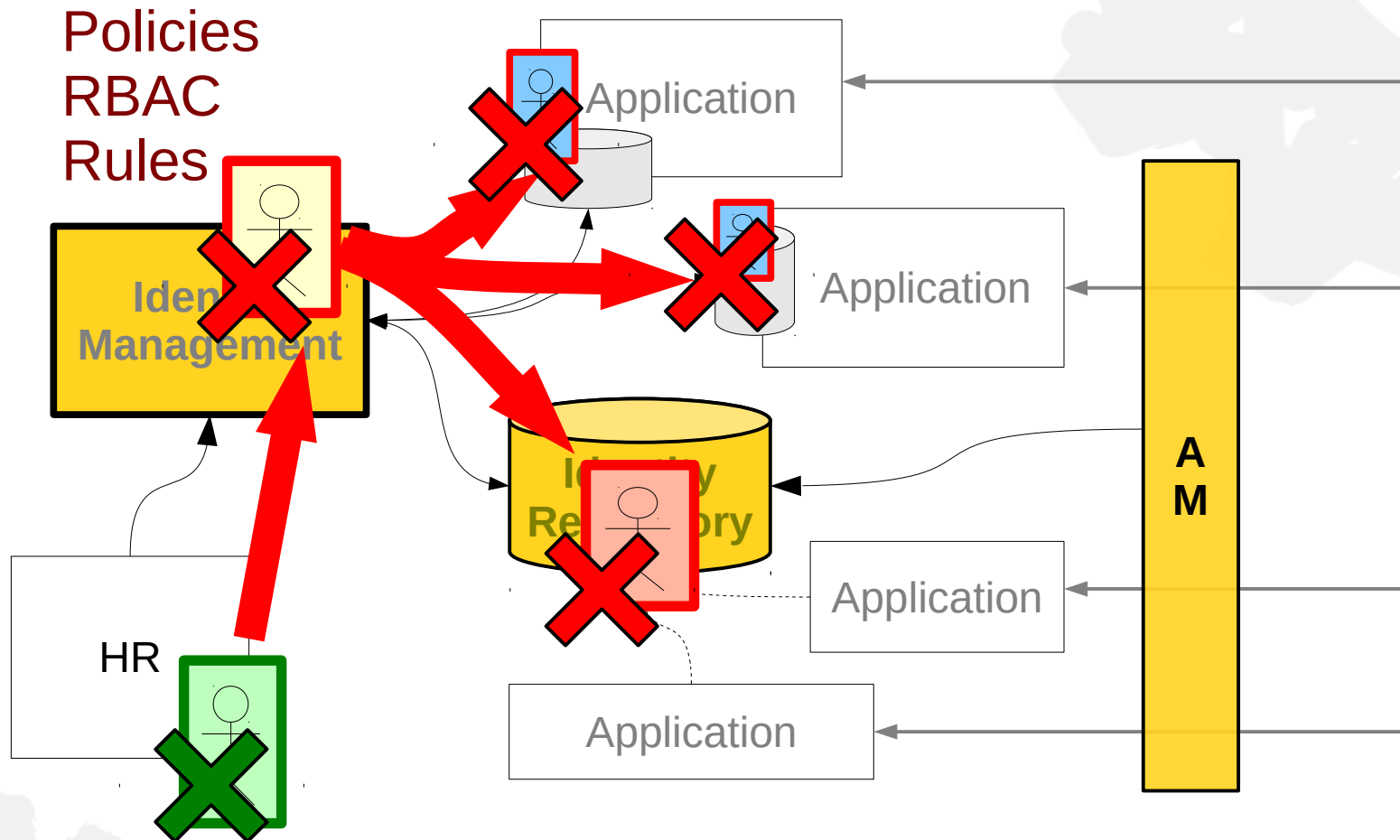
Password reset (self-service)



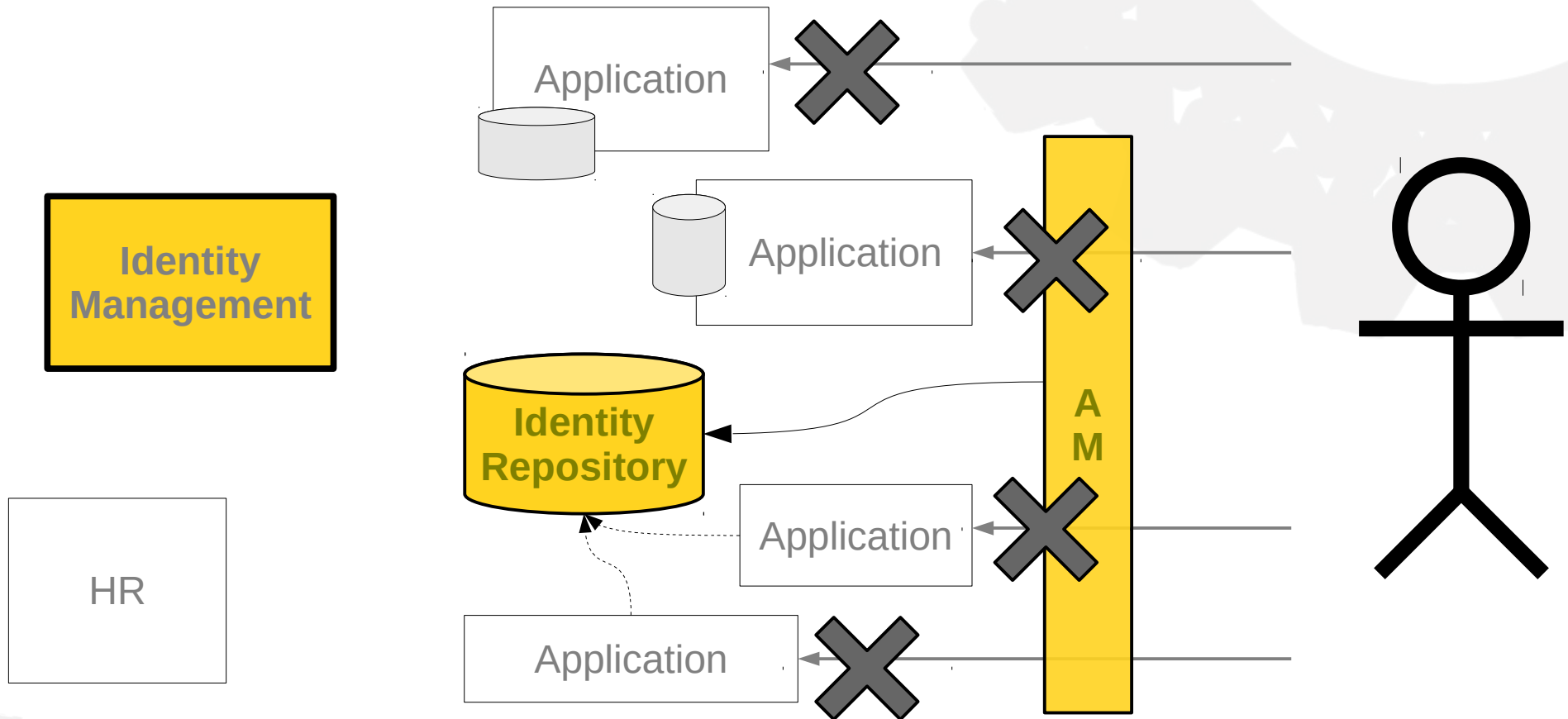
Employee Leaves Company



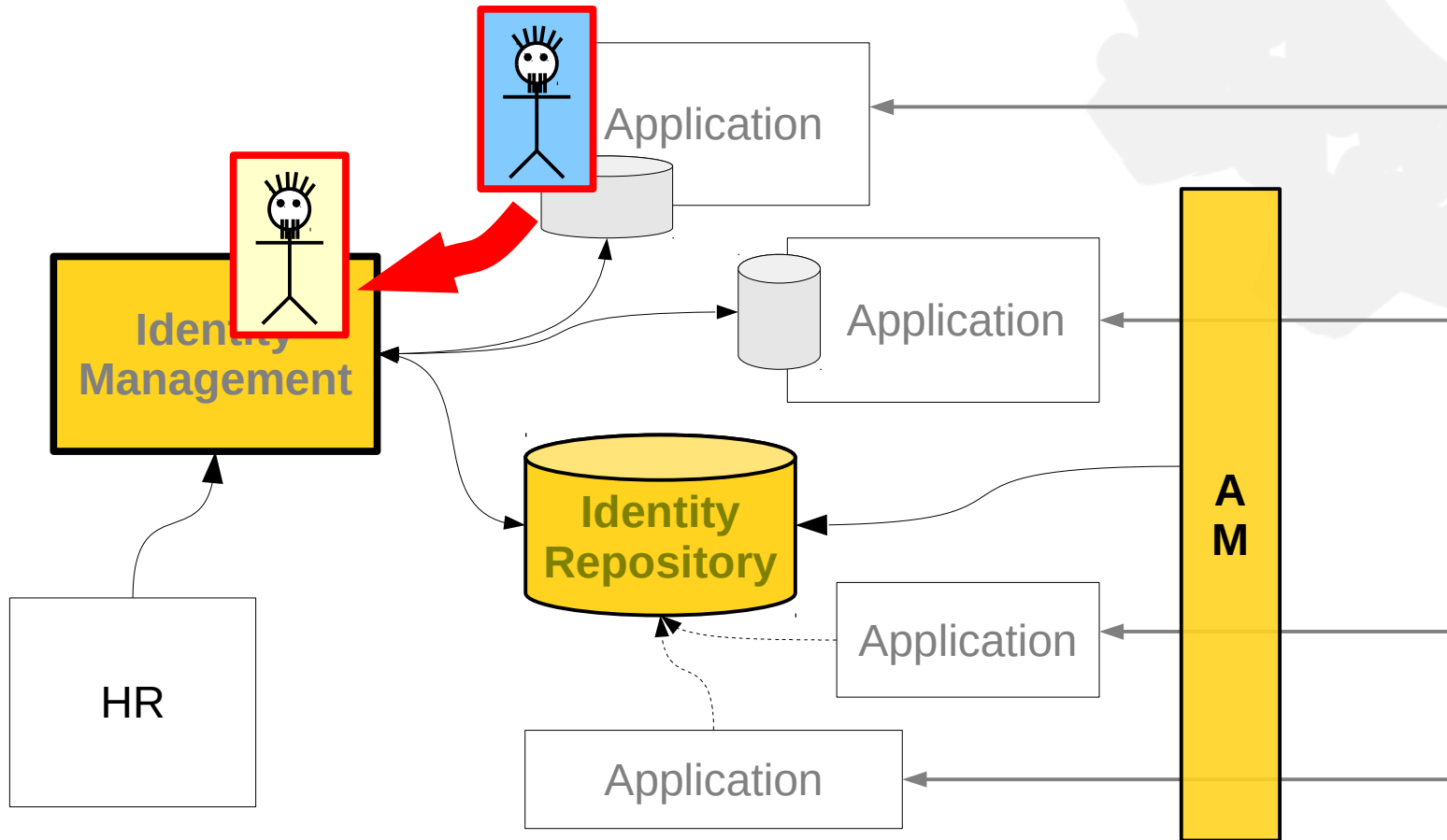
Automatic user deprovisioning



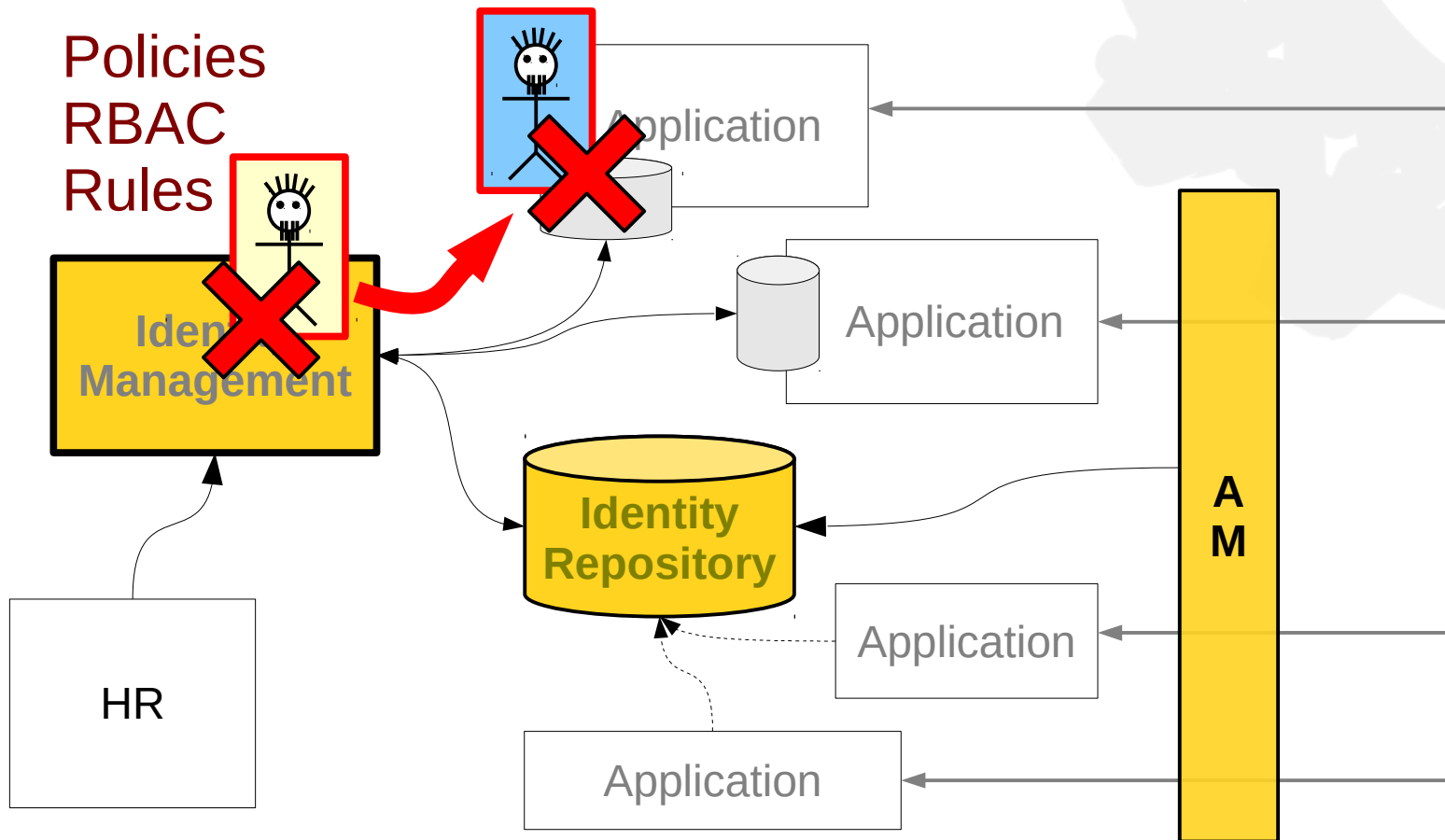
Business As Usual



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
- ...



Leonardo da Vinci (leonardo)

✔ Active

Department of Machines

Basic

Details



Name *

Full Name

Given Name

Family Name

Nickname

Telephone Number

Employee Number

Employee Type +

Jpeg photo No file selected + - x

Extension

Artistic Name ⓘ

Activation

Administrative Status

Password

Password Change

Projections



HR Feed default, 1

Addressbook default, leonardo

LDAP Server (OpenLDAP) over new LDAPConn.
default, uid=leonardo,ou=People,dc=example,dc=com

Organizations

Department of Machines F0200

Smile P0001

Assignments



F0200 -

P0001 -

Full Time Employee -

Patron -

HR Feed -

SELF SERVICE

- Home
- Profile
- Credentials

ADMINISTRATION

- Dashboard
- Users
- Org. structure**
- Organization tree
- New organization
- Roles
- Resources
- Work items
- Server tasks
- Reports
- Configuration

Org. structure tree

Projects Leonardo's Workshop

Subtree

Org. hierarchy

- Leonardo's Workshop
 - Department of Arts
 - Painting Lounge
 - Sculpting Corner
 - Department of Machines
 - War Machines Section

Children org. units

<input type="checkbox"/>	Name	Display name	Identifier
<input type="checkbox"/>	F0210	War Machines Section	0210

Displaying 1 to 1 of 1 matching result.

Managers

<input type="checkbox"/>	Name	Given name	Family name	Full name	Email
No matching result found.					

Members

<input type="checkbox"/>	Name	Given name	Family name	Full name	Email
<input type="checkbox"/>	leonardo	Leonardo	da Vinci	Leonardo da Vinci	

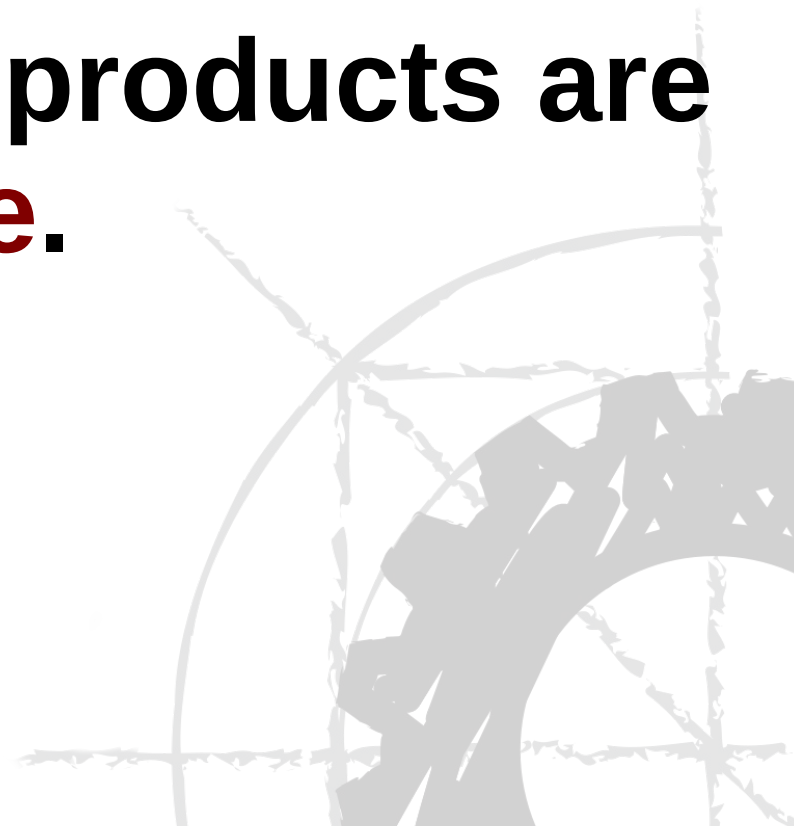
Displaying 1 to 1 of 1 matching result.

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

But ... there was no practical FOSS solution

The market was taken by

Sun, Oracle, IBM, CA, Microsoft, SAP, ...

(money, money, money)

Open Source to the Rescue

2010-2011

We have started

one developer, two developers, three developers, ...

bumpy start (details in the blog)

by mid-2011 fully operational

2011

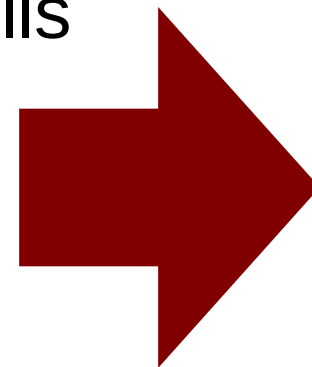
Evolveum

Good architecture, code base, skills

No real business plan

No customers

Big, rich, established competitors



**foolishly
naïve
lunacy**

2011-2014

Evolveum

hard work

no money

2015-2016

Evolveum

success

and beyond

Evolveum



money

No big investor, only FFF (Friends, Family, Fools)

Key employees receive shares from profit

Early income: anything (really)

Current income: subscriptions and professional services

2015: (small) profit

Evolveum



technology

Small team (5 developers + 2 engineers)

Efficiency: Java, formal data model, generated code

Cooperation: ConnId, Apache Directory API

Developer freedom: no bosses, pet projects, ...

Experiments: LDAP, GUI, OpenStack, ...

Great Technology in MidPoint

- Java, Spring, Apache Wicket (nothing special here)
- Good architecture from day one
- Internal scripting: Groovy, JavaScript, Python
- Self-healing system
- Prism Objects
- Advanced Hybrid RBAC
- ...

Prism Objects

Schema

```
complexType: UserType  
  element: givenName  
  element: fullName  
  ...
```

Code

```
class UserType {  
  String givenName;  
  String fullName;  
  ...  
}
```

XML, JSON, YAML

REST

SOAP

```
<wsdl>...</wsdl>
```

GUI

User details

Given name:

Full name:

Cancel

Save



Leonardo da Vinci (leonardo)

✓ Active

Department of Machines

Basic

Details



Name *

Full Name

Given Name

Family Name

Nickname

Telephone Number

Employee Number

Employee Type

Jpeg photo No file selected

Extension

Artistic Name ⓘ

Activation

Administrative Status

Password

Password

Projections



HR Feed default, 1

Addressbook default, leonardo

LDAP Server (OpenLDAP) over new LDAPConn.

default, uid=leonardo,ou=People,dc=example,dc=com

Organizations

Department of Machines F0200

Smile P0001

Assignments



F0200 -

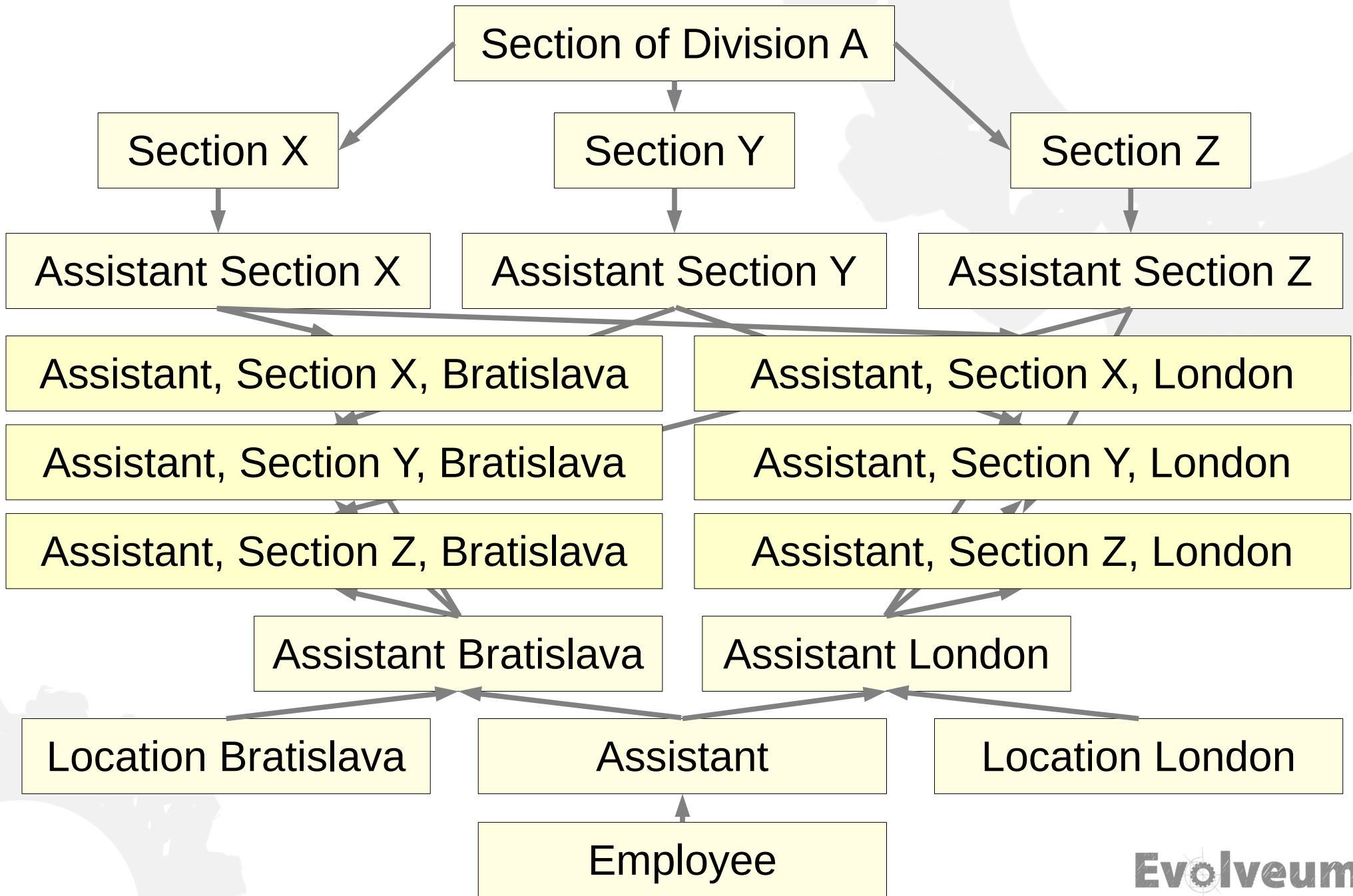
P0001 -

Full Time Employee -

Patron -

HR Feed -

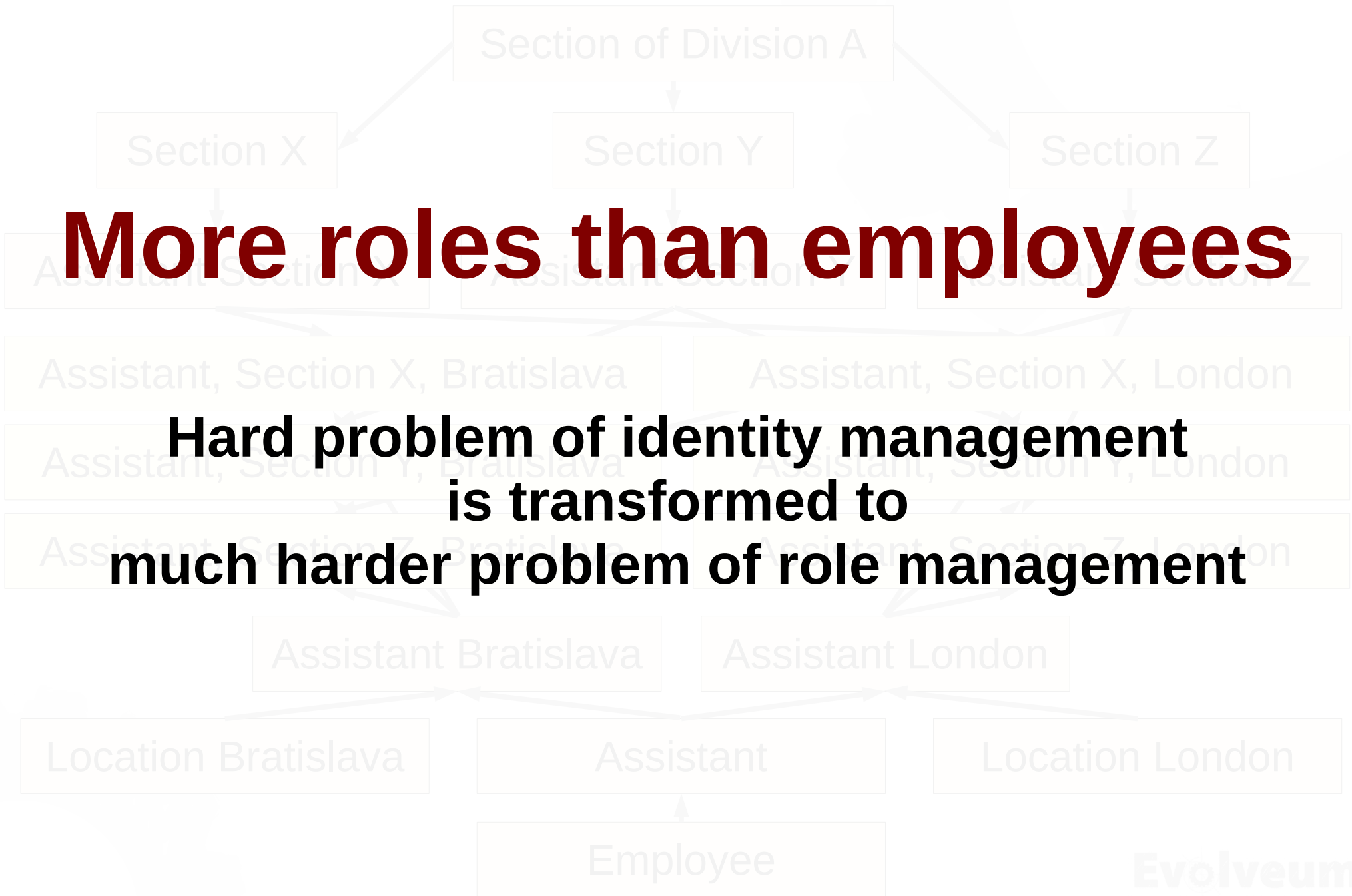
Classic RBAC → Role explosion



Classic RBAC → Role explosion

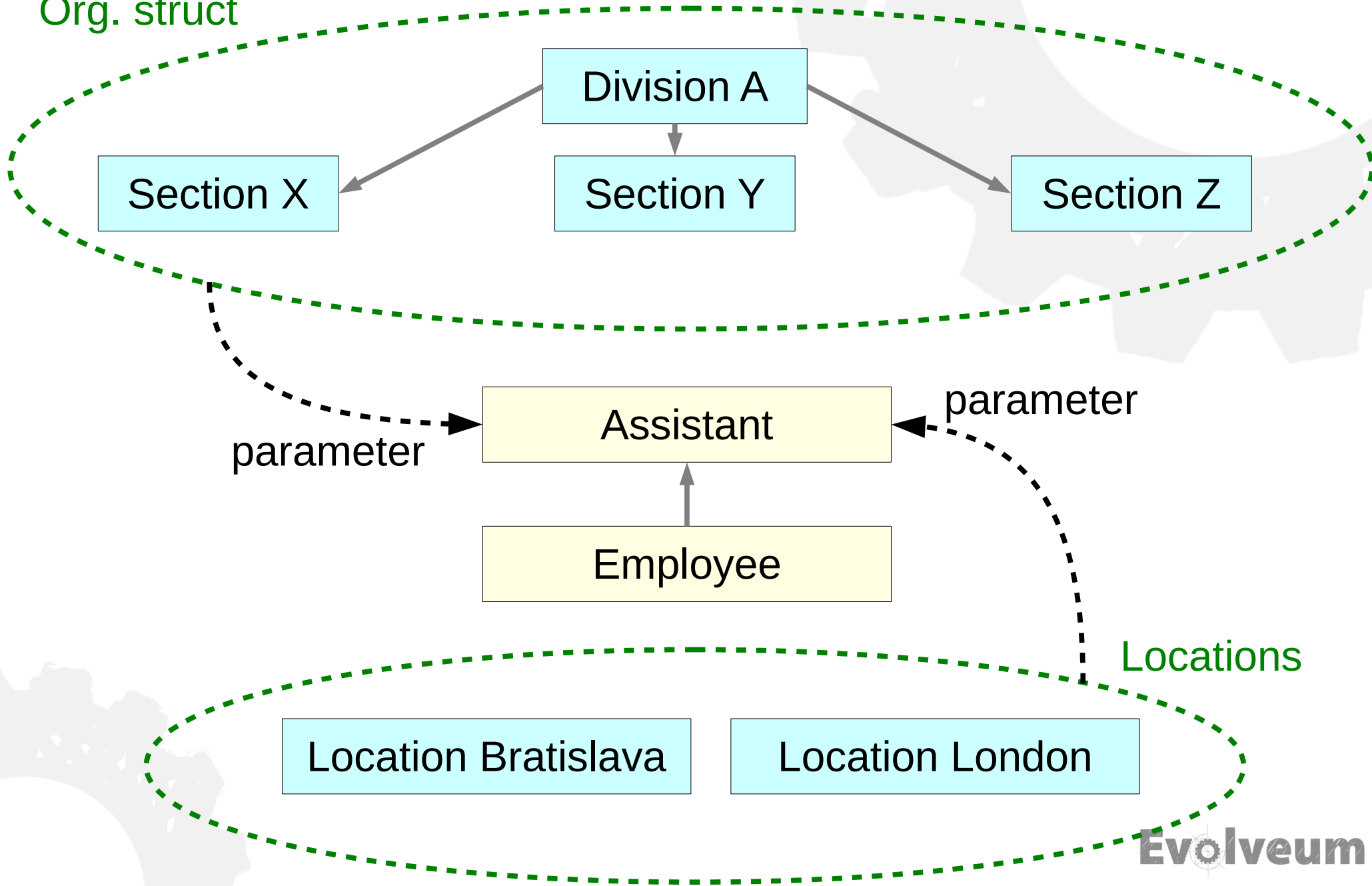
More roles than employees

**Hard problem of identity management
is transformed to
much harder problem of role management**



MidPoint Advanced Hybrid RBAC

Org. struct



Evolveum



success

Most comprehensive open source IDM system

Great engineering team, great technology

Recognized by analysts (Gartner, KuppingerCole)

World-wide adoption

Successfully competing with Oracle, IBM, Microsoft, ...

Lessons learned

- Forget about Slovakia. World is your market!
- Efficiency: Small team, big impact
- Burn money slowly. Wait for the right moment.
- Do not look for customers, let customers look for you.
- Technology matters. A lot. Really.
- Good platform and architecture is crucial
- Newest technology is not always coolest

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

Thank You

Radovan Semančík

www.evolveum.com