

Identity Management with midPoint



Radovan Semančík
FOSDEM, January 2016

Radovan Semančík



Current:

Software Architect at **Evolveum**

Architect of Evolveum **midPoint**

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

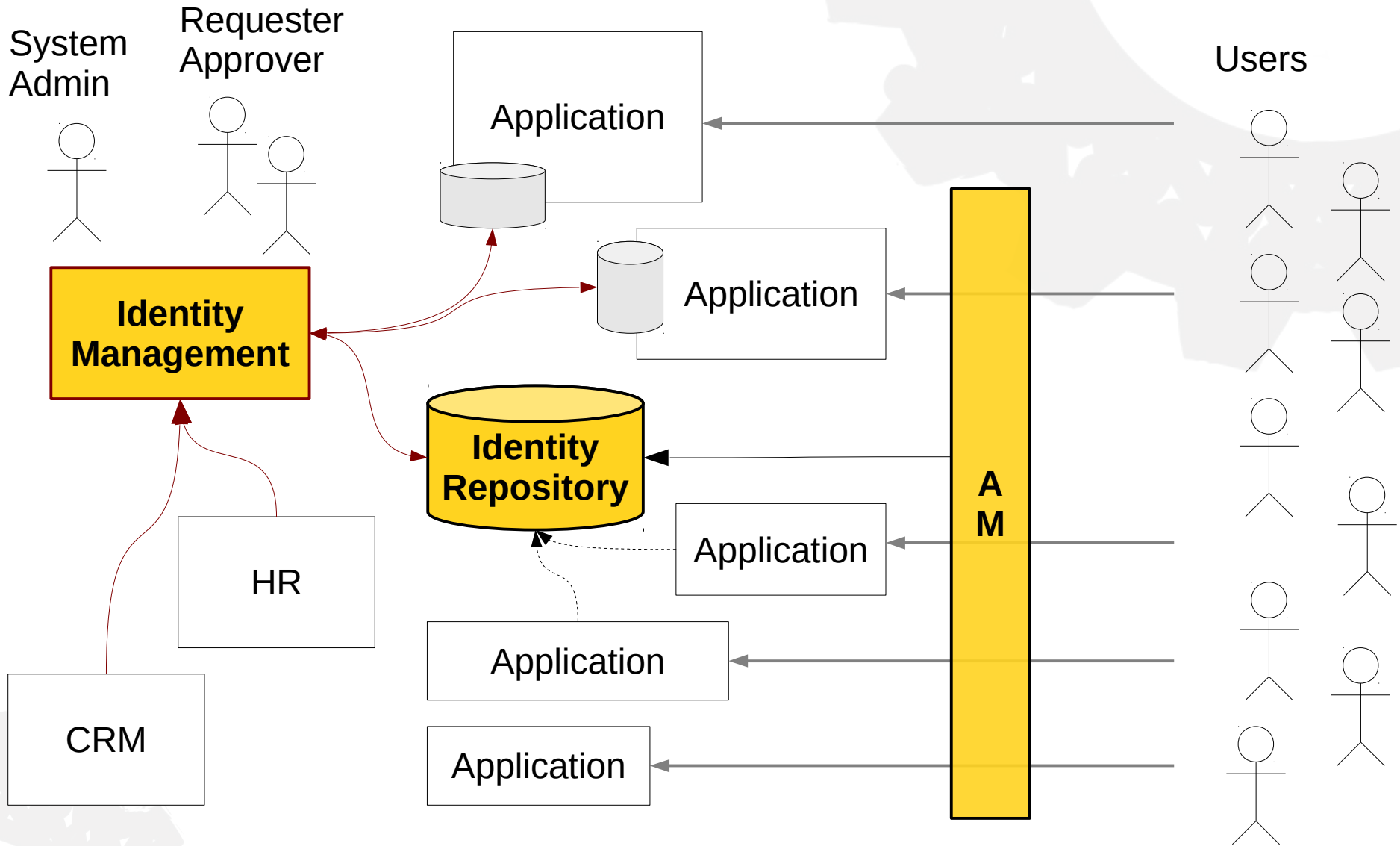
Past:

Sun LDAP and IDM deployments (early 2000s)

OpenIDM v1, OpenICF

Many software architecture and security projects

Identity and Access Management






There is **no security** without
identity management

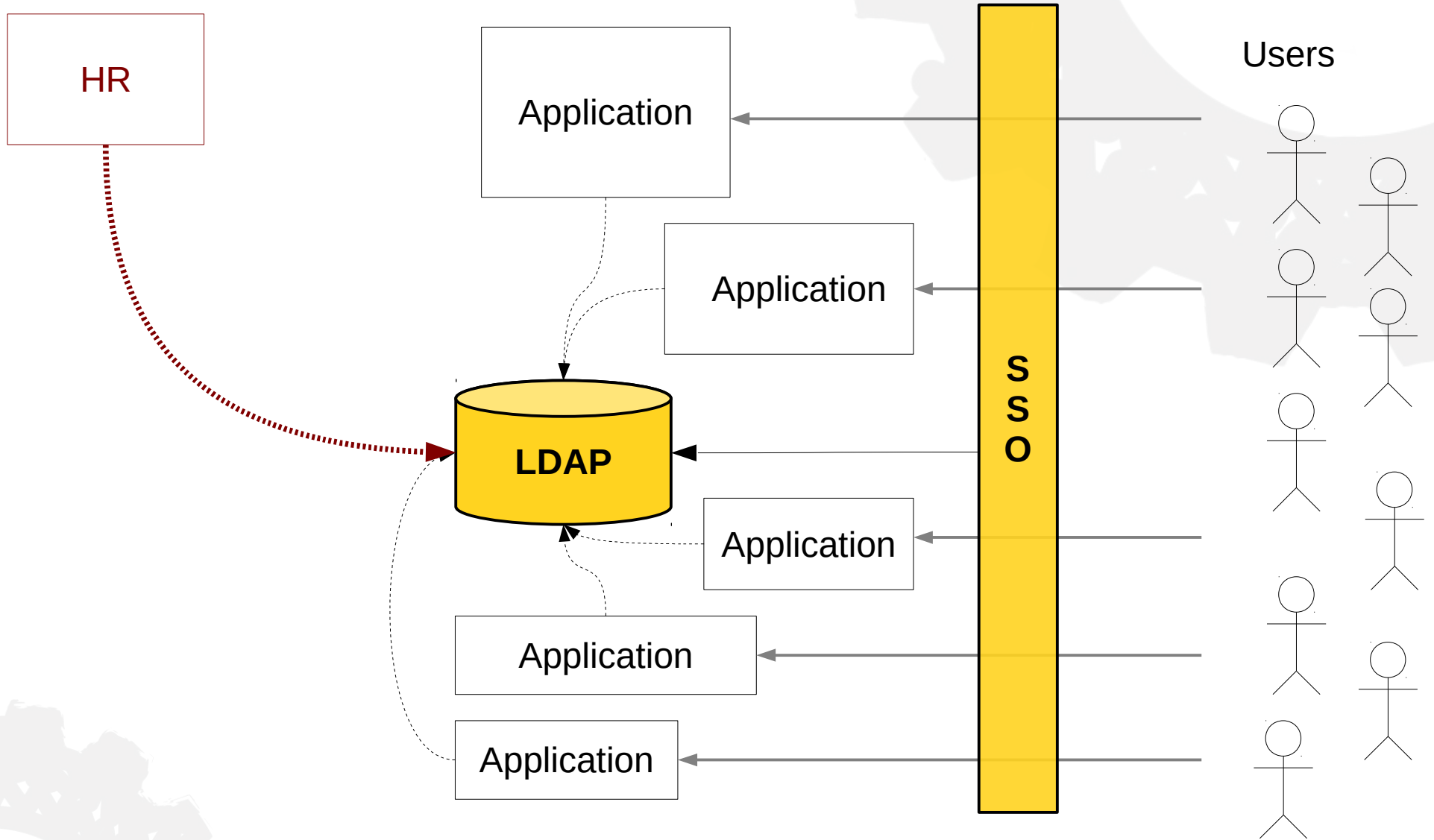
If you have no IDM, how can you be sure that ...

- 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?

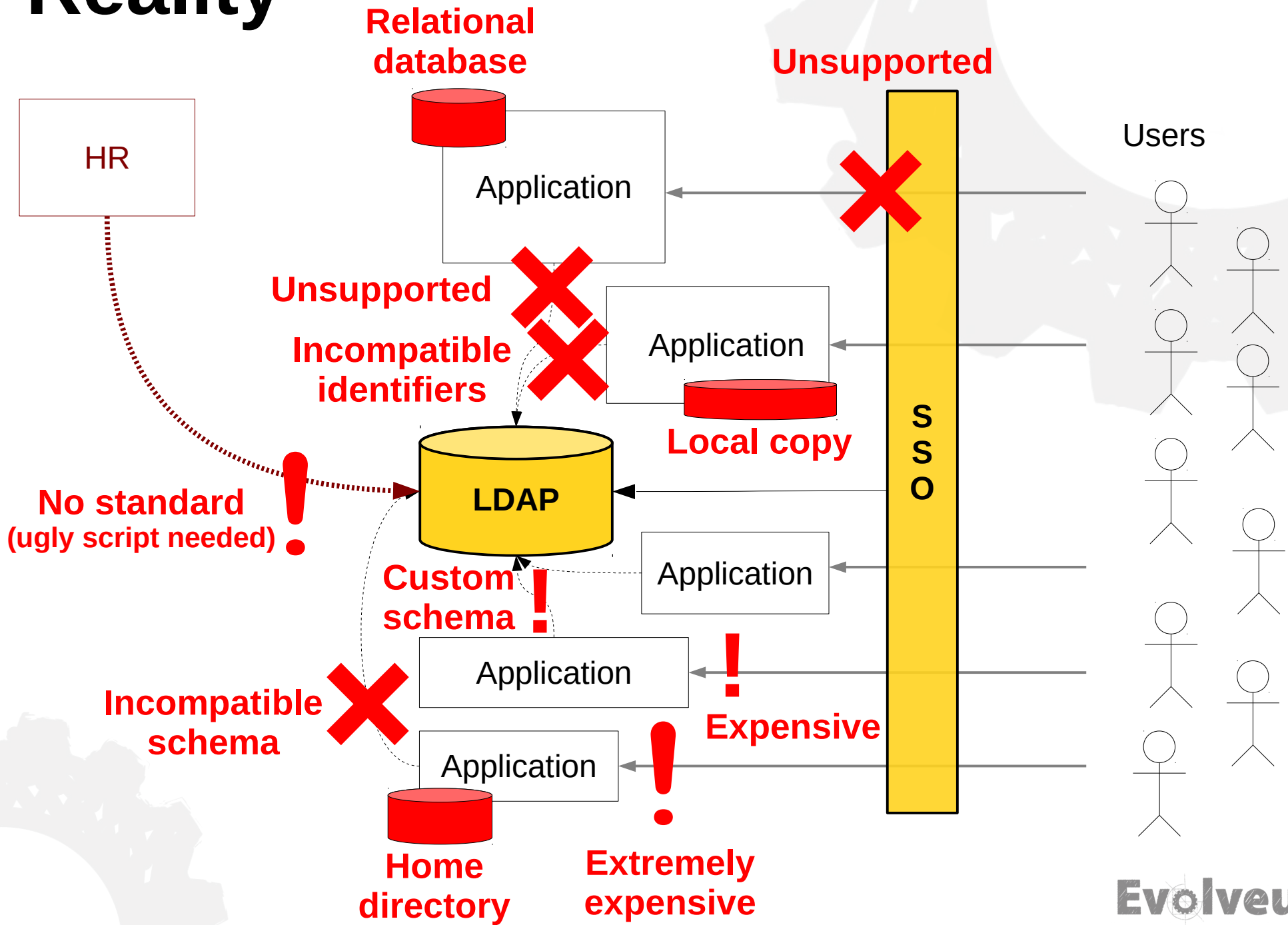


The solution is trivial
Let's put everything in LDAP!

Expectation



Reality

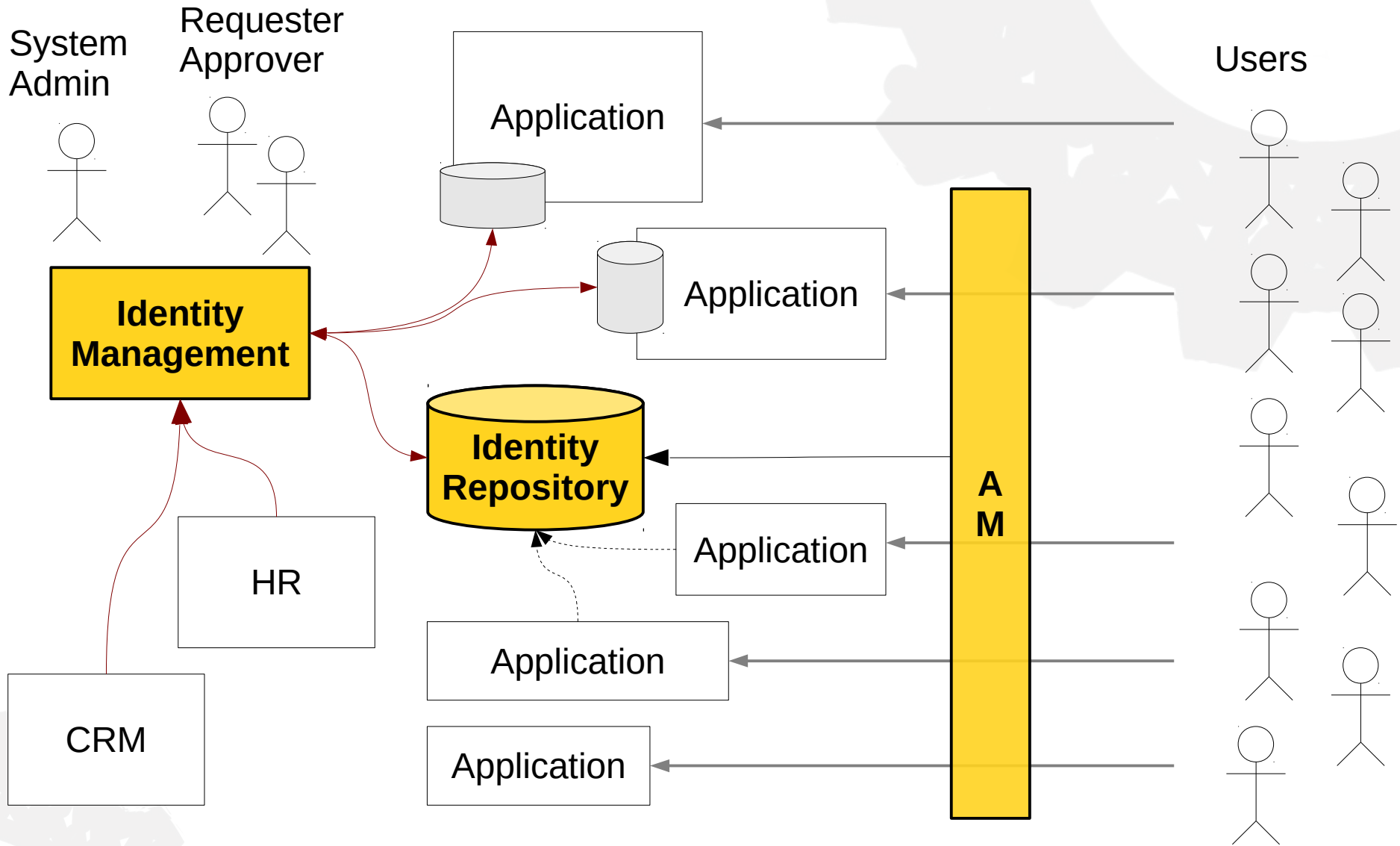




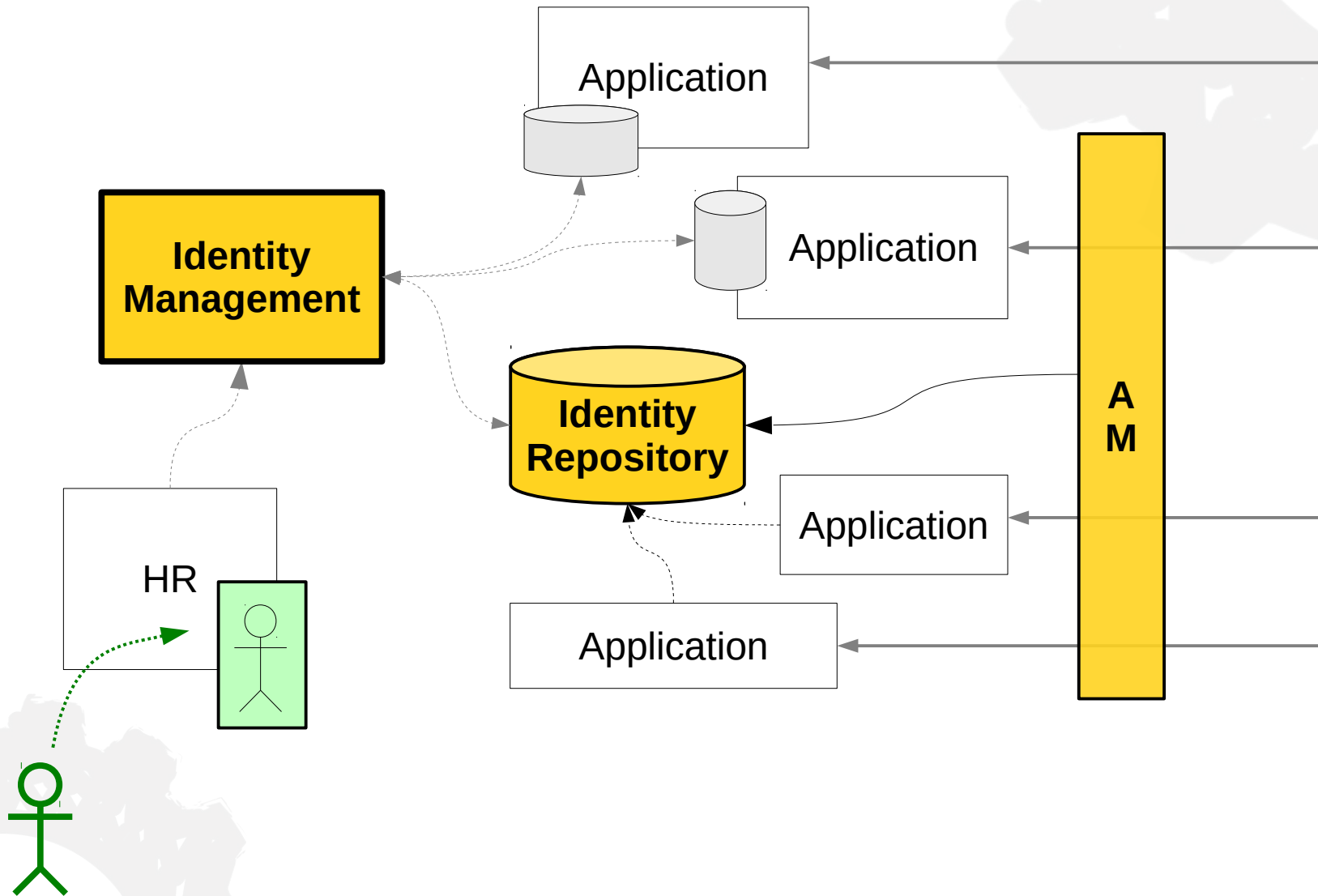
“Single directory” approach is **not going to work**

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

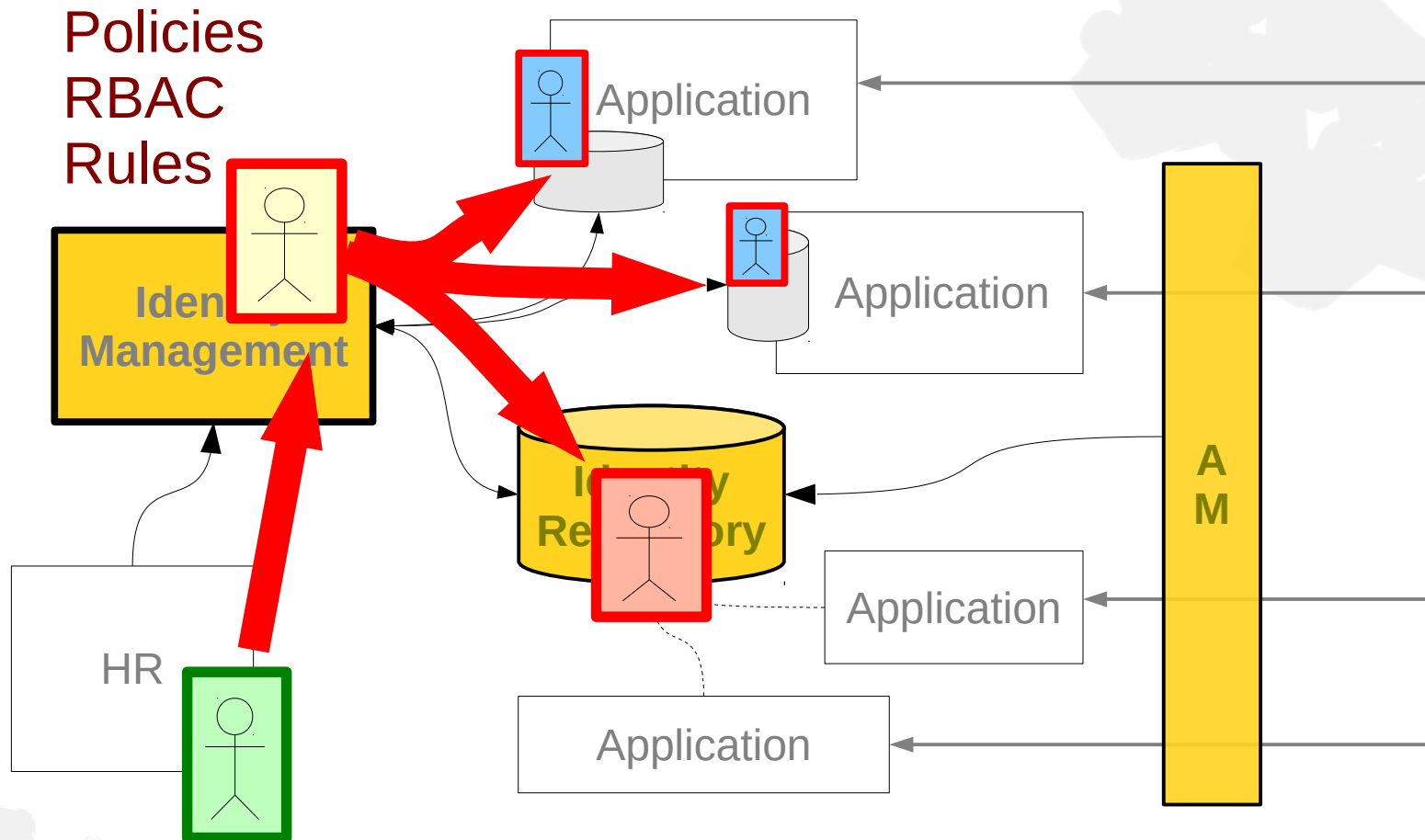
Identity and Access Management



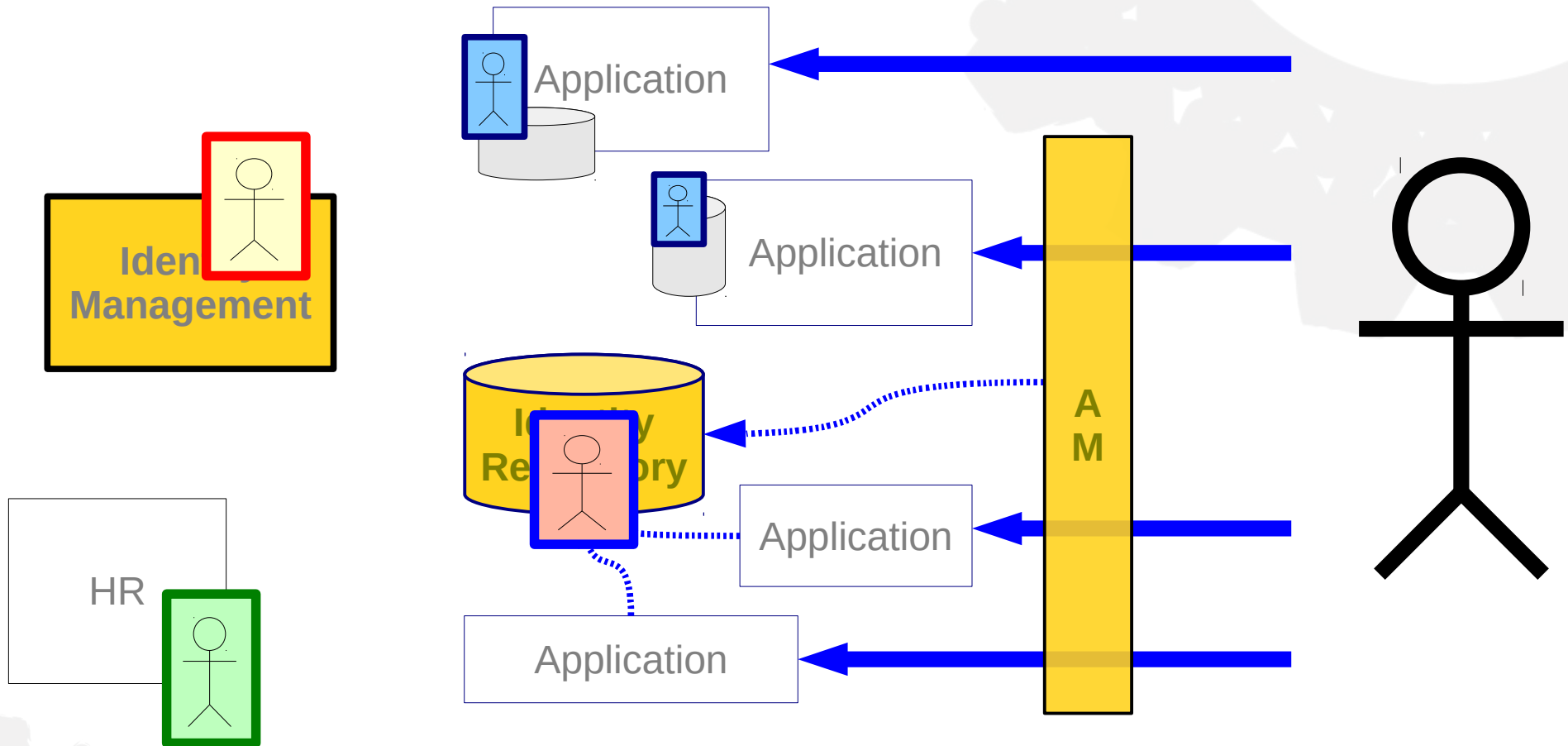
How IDM works?



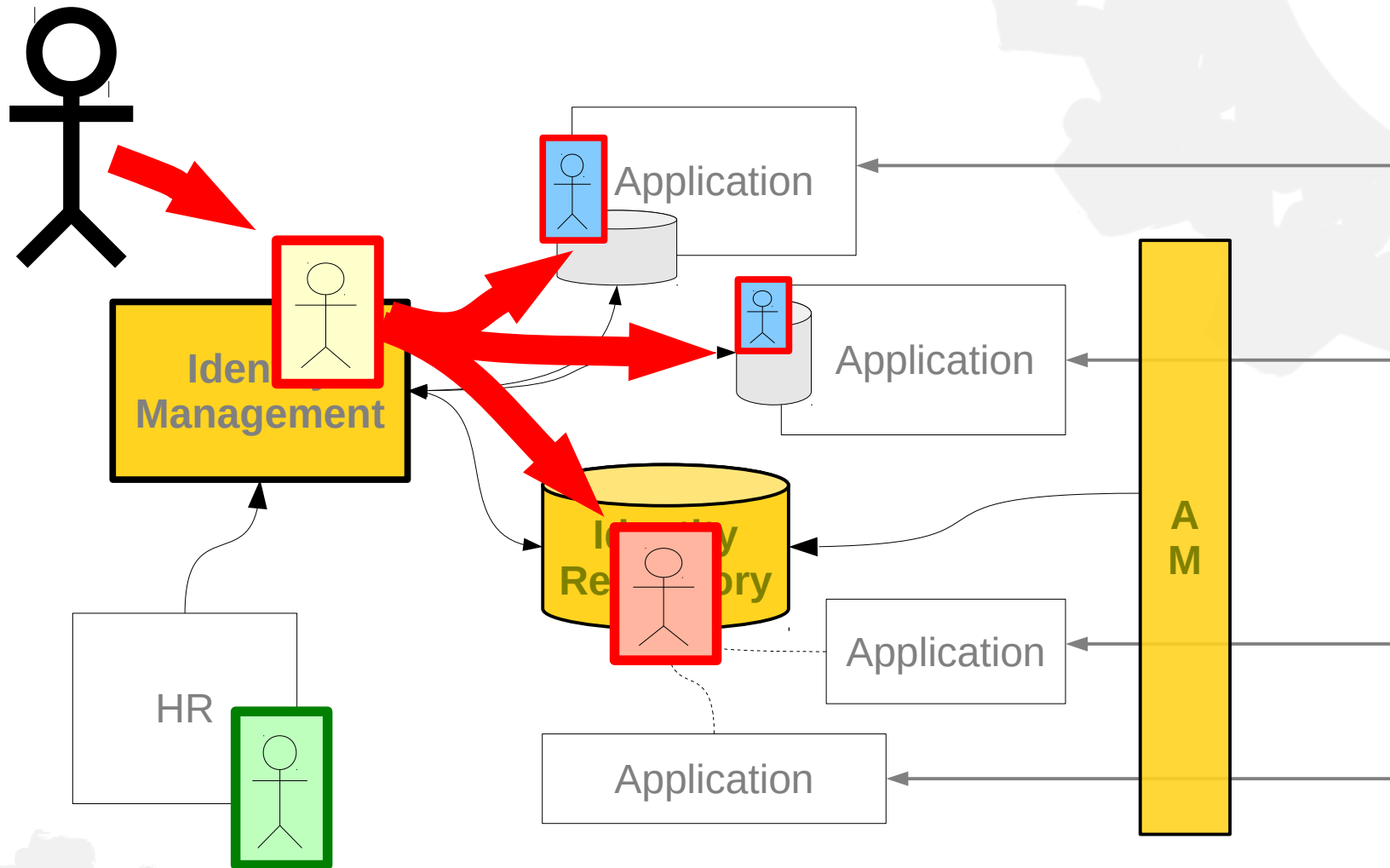
Automatic user provisioning



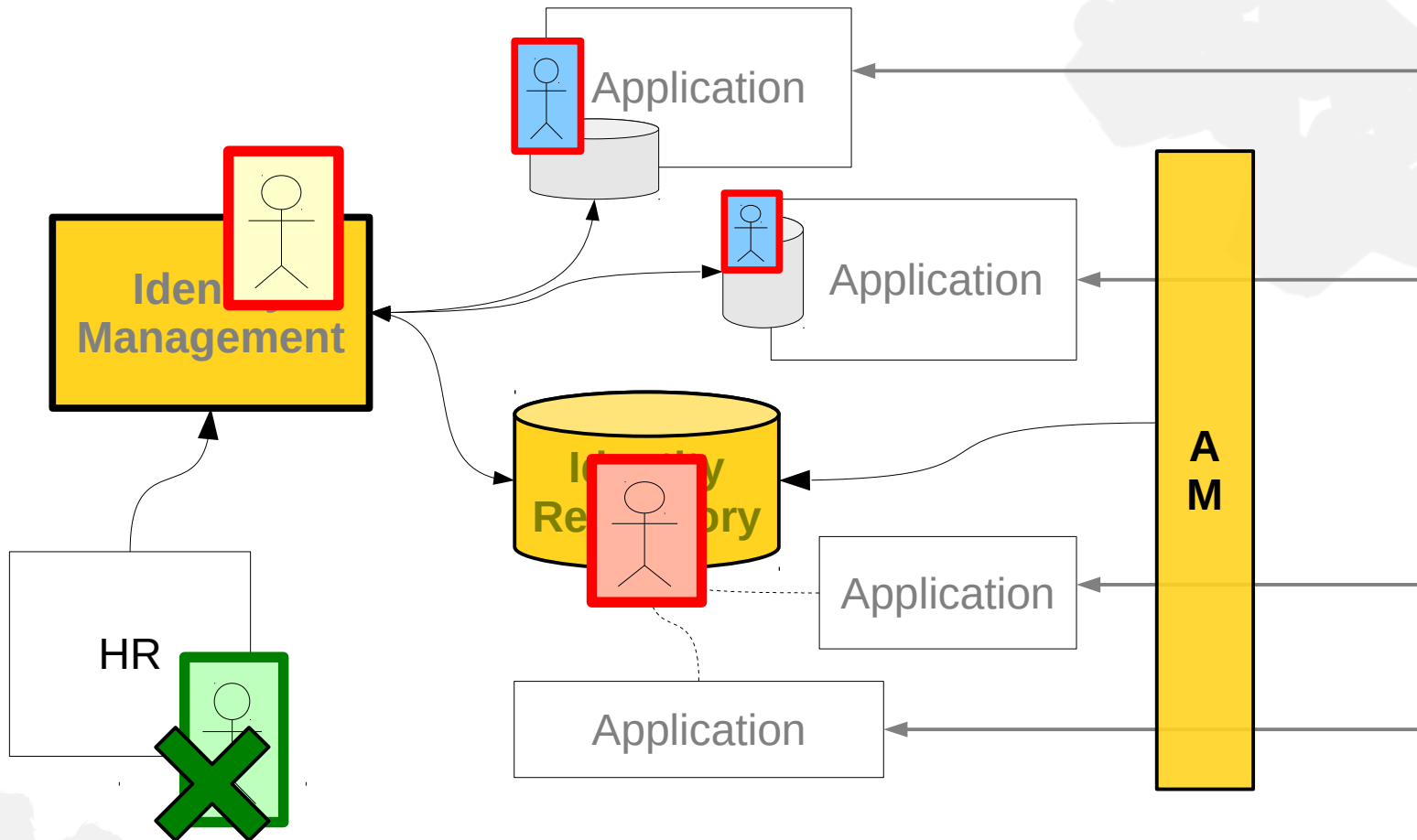
Business As Usual



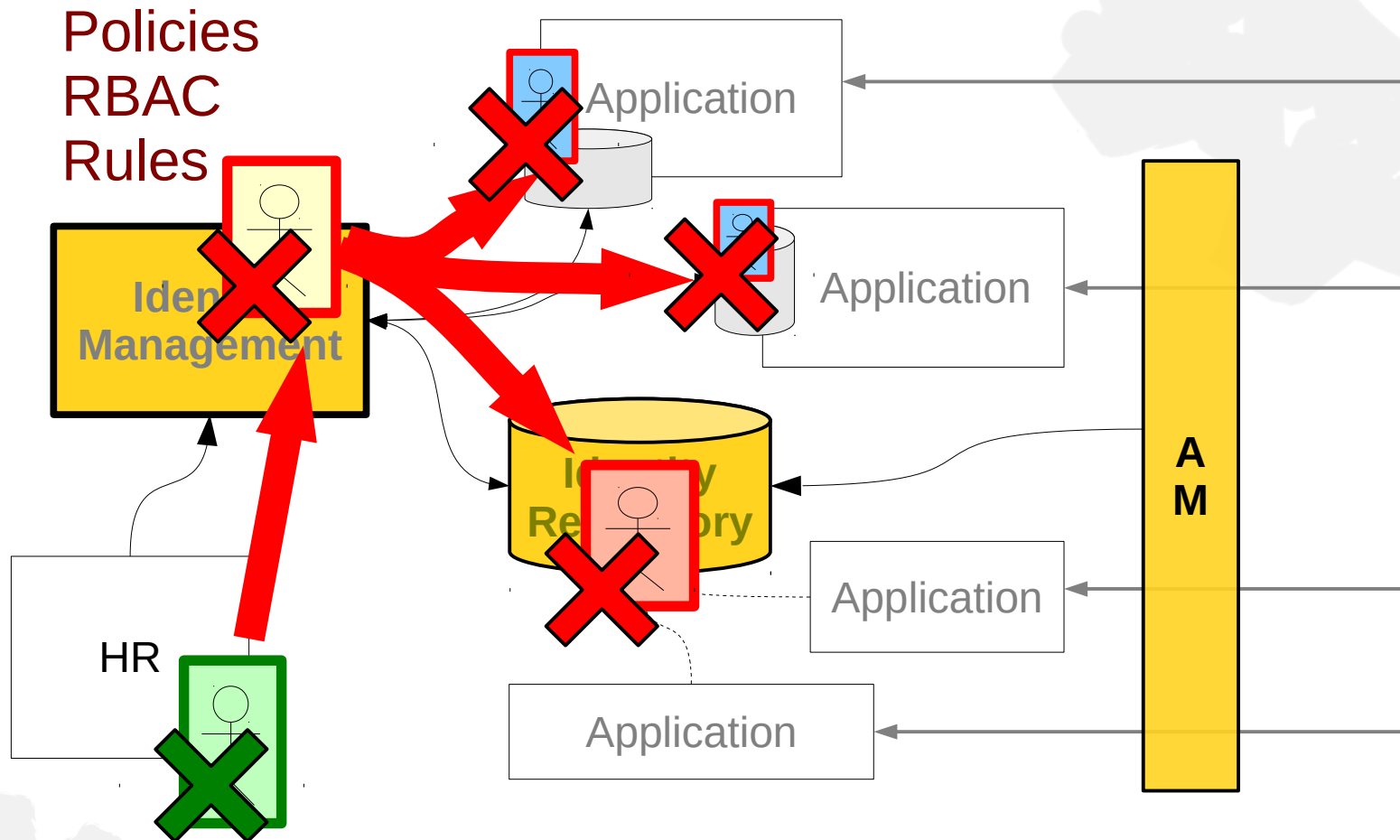
Password reset (self-service)



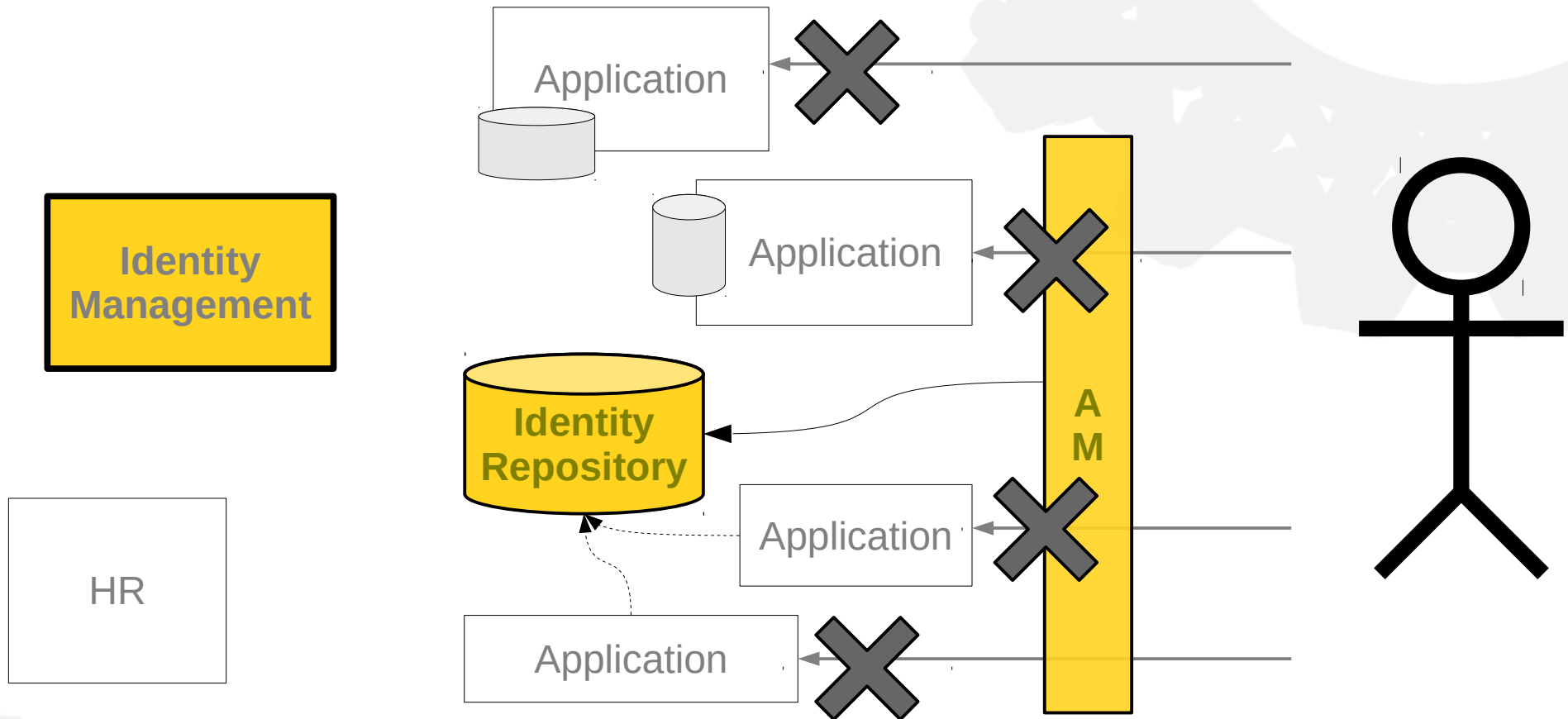
Employee Leaves Company



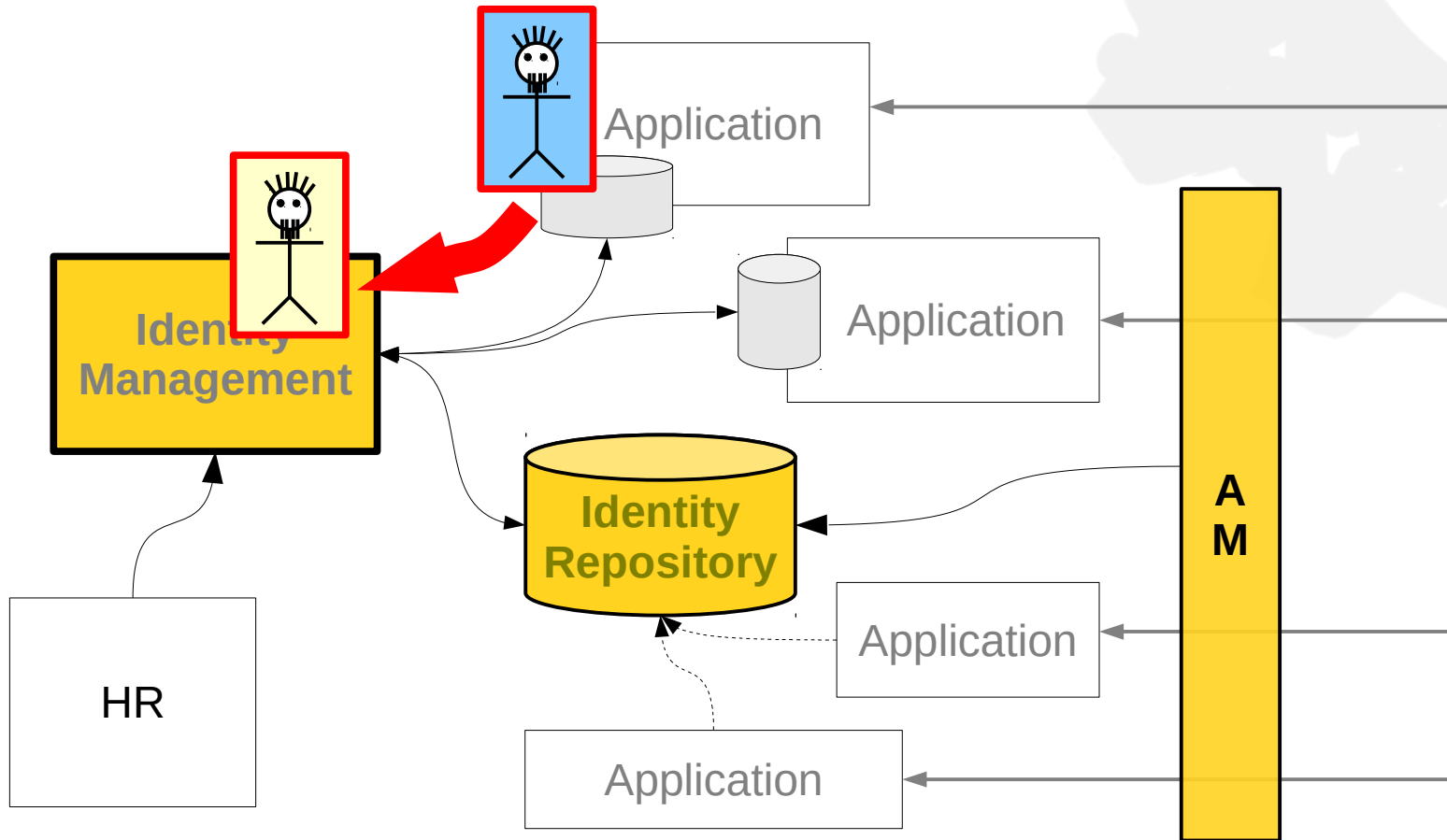
Automatic user deprovisioning



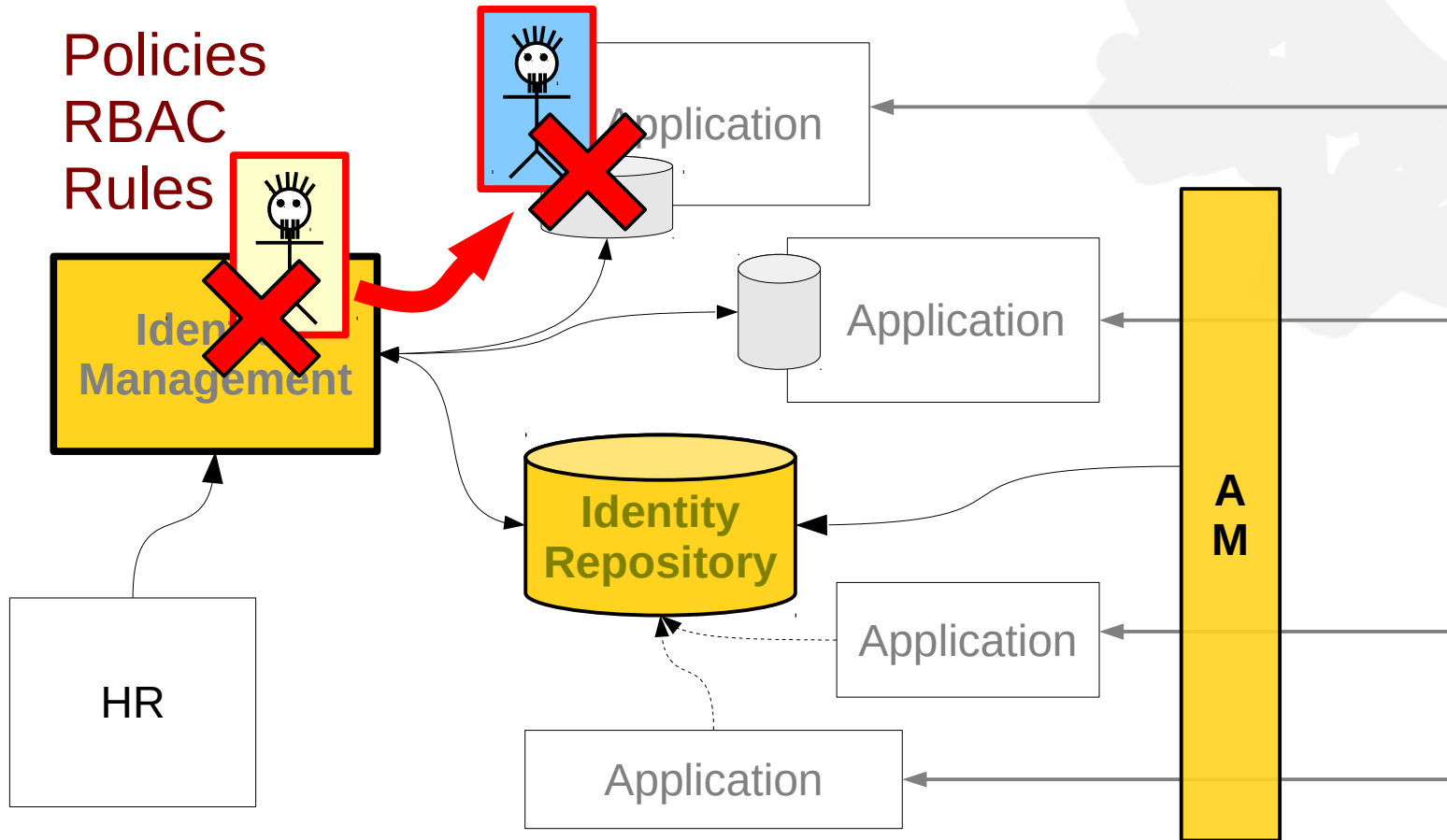
Business As Usual



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
- ...

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:

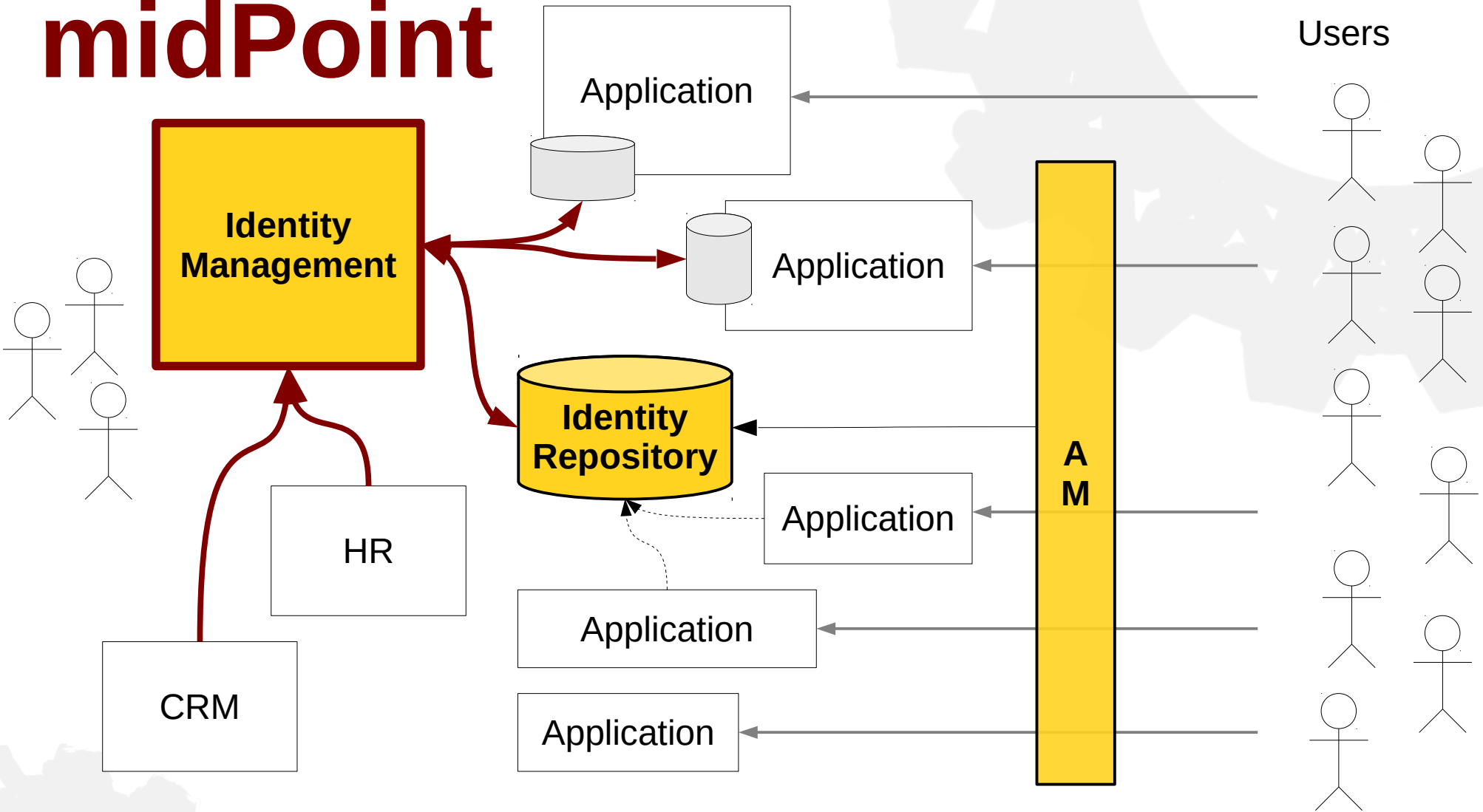
- **Apache Syncope**
- **Evolveum midPoint**

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



Evolveum midPoint?

midPoint



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 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



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 -

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"/>
<input type="checkbox"/>	F0210	War Machines Section	0210	<input type="checkbox"/>

Displaying 1 to 1 of 1 matching result.

Managers

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

Members

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

Displaying 1 to 1 of 1 matching result.

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