Introduction to Identity and Access Management

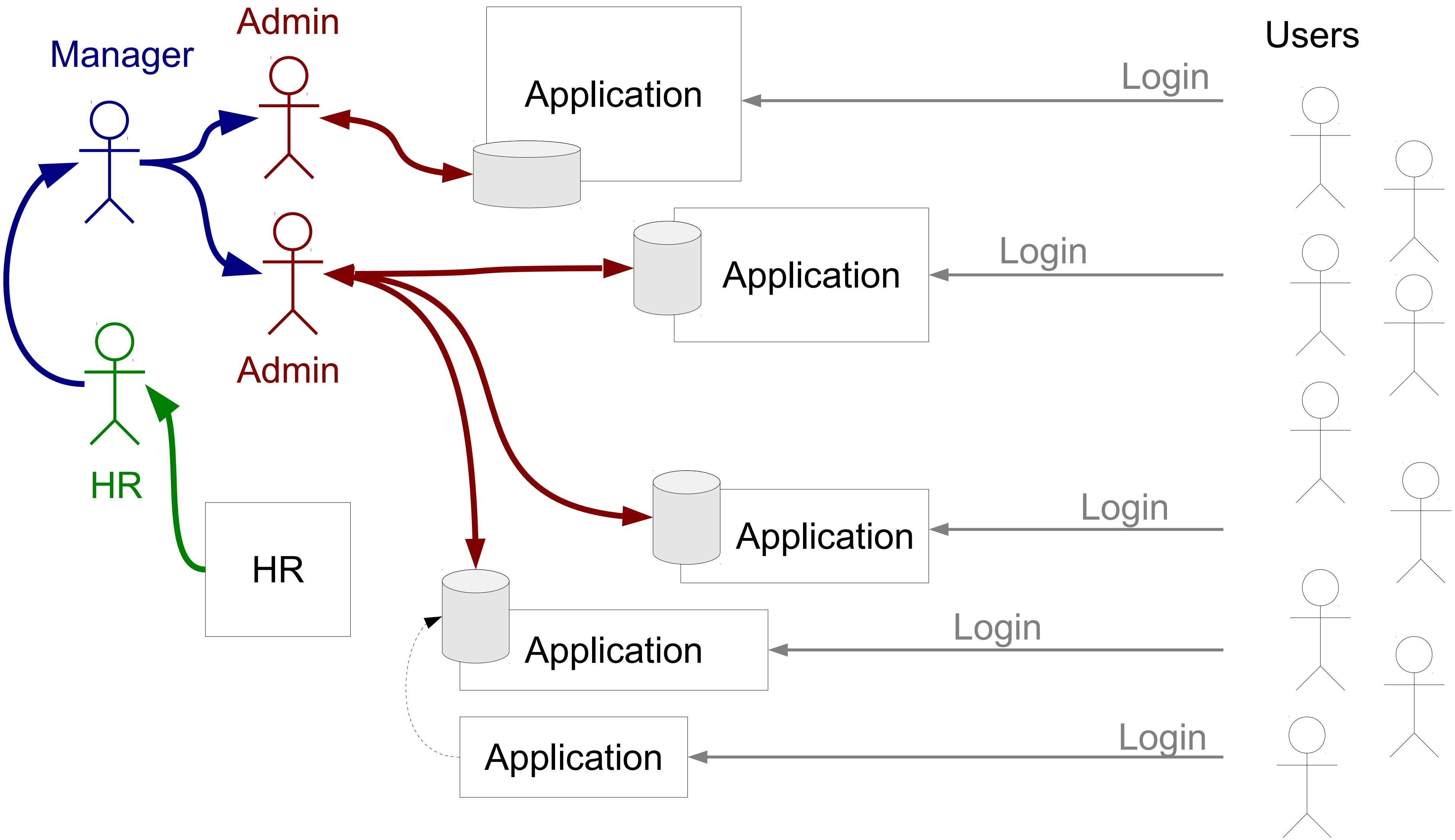
for the engineers

Evolveum

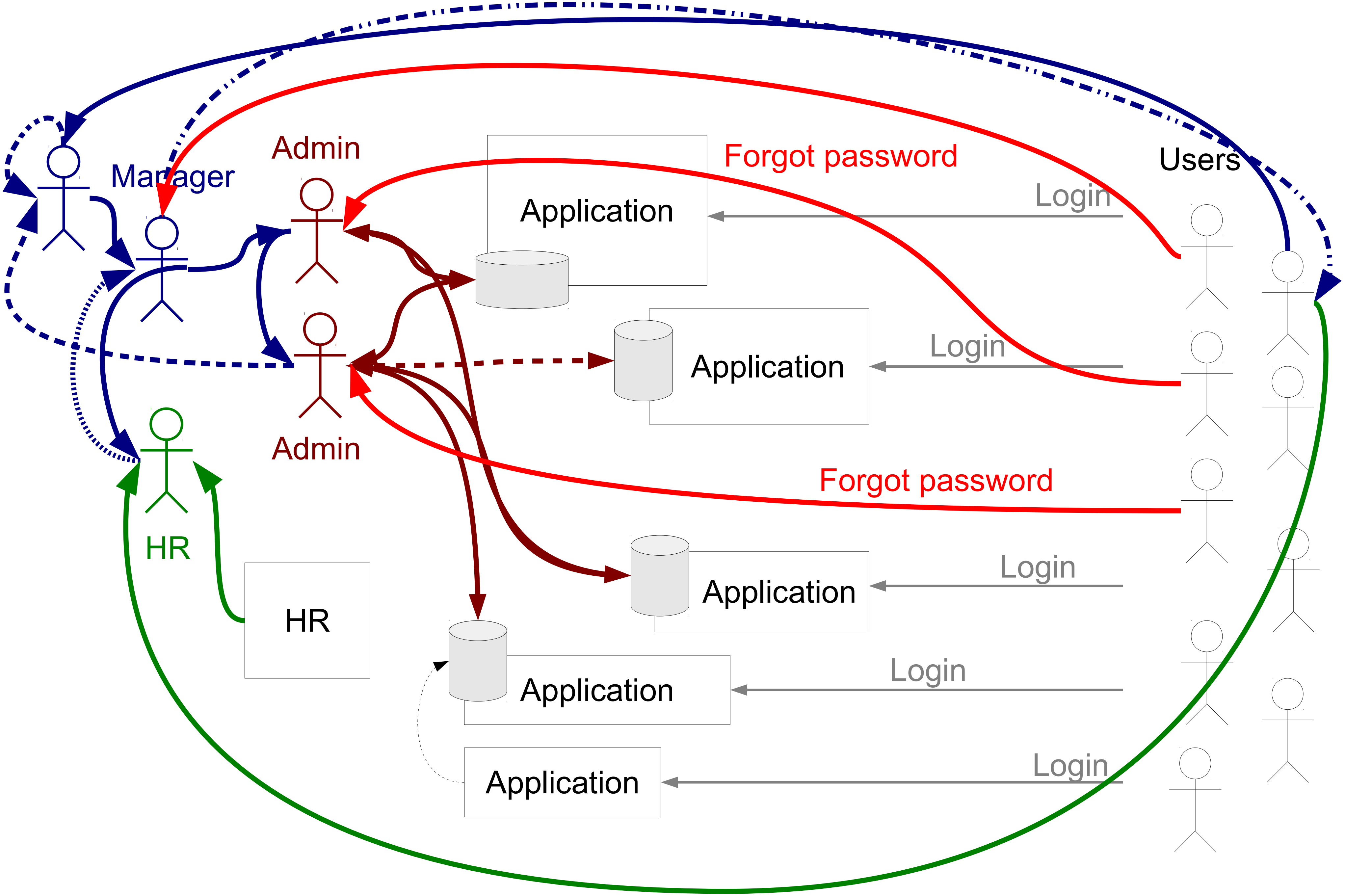
Radovan Semančík

April 2014

How it works now?

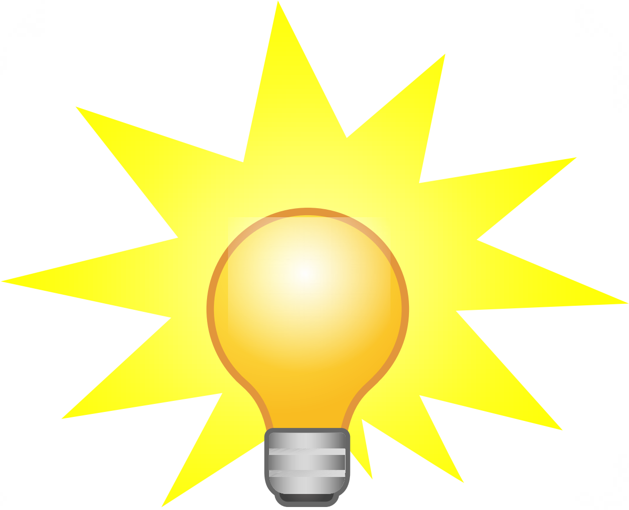

Manager
Admin
Admin
HR
HR
Application
Application
Application
Application
Application
Users
Login
Login
Login
Login
Login

Theory

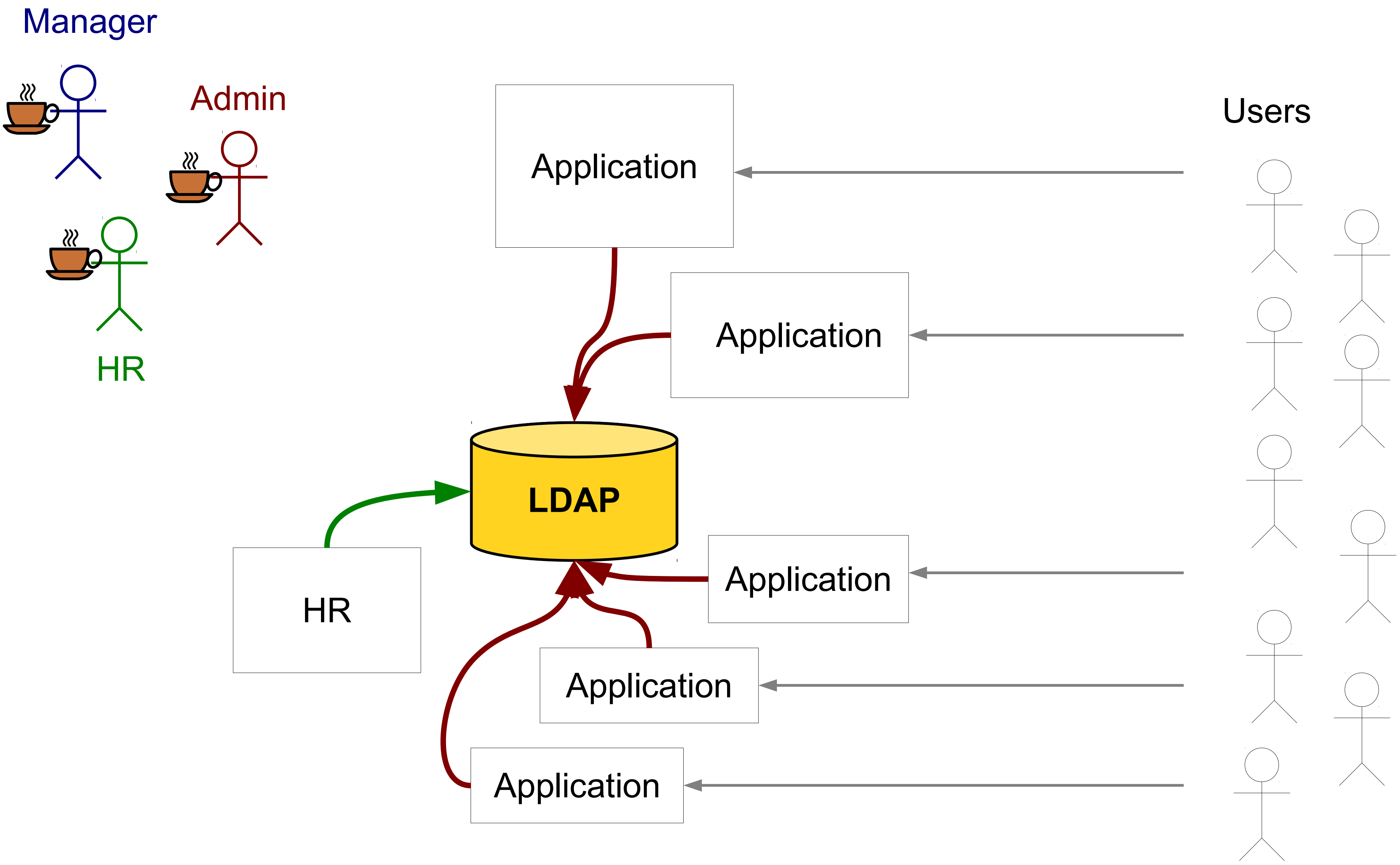

Admin
Manager
Forgot password
Users
Application
Login
Application
Login
Admin
Forgot password
HR
Application
Login
HR
Application
Login
Application
Login

Practice

Idea: Let's deploy LDAP!



Theory



Manager

Admin

HR

Application

Application

LDAP

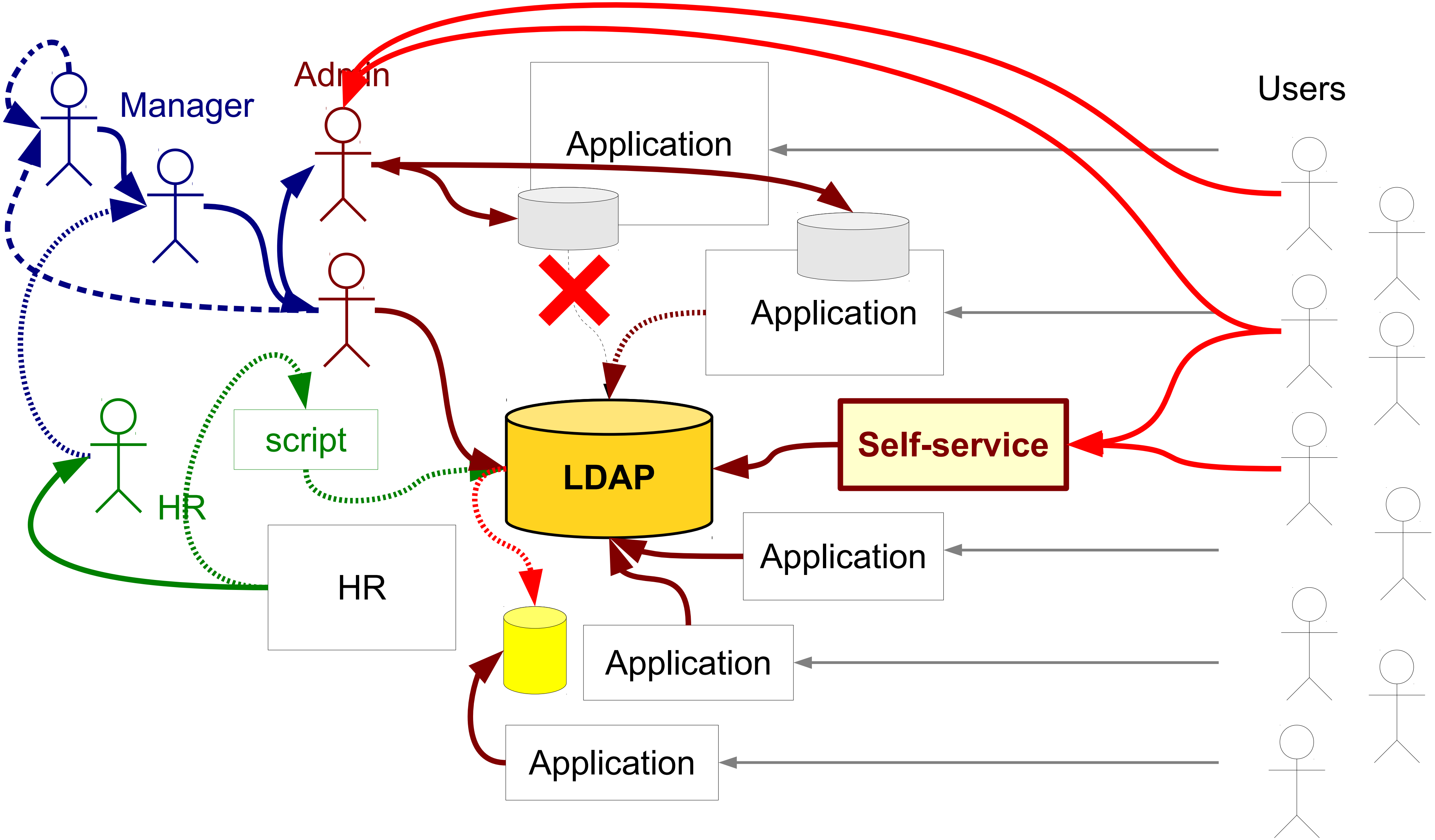
HR

Application

Application

Application

Users


Manager
Admin
Users
Application
Application
script
LDAP
Self-service
HR
HR
Application
Application
Application

Practice

Why?

Because some applications …

- just don't support LDAP
- support LDAP but still need local account
- require incompatible schema
- require complex policies (LDAP is simple)

There is more than one data source

- HR, CRM, AIS, manual, ...

LDAP is (too) simple!

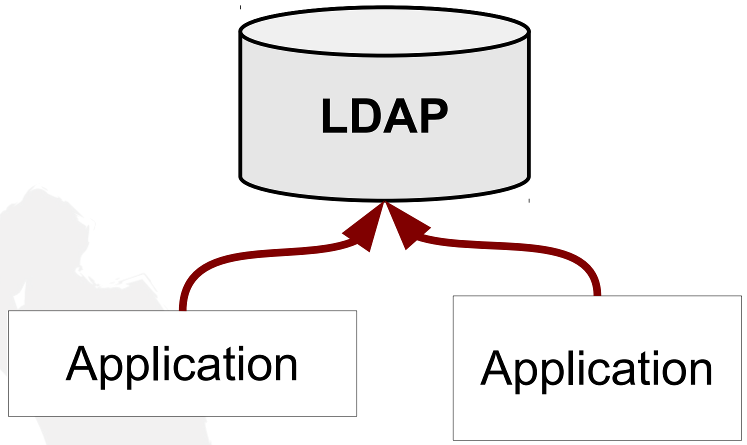
- It is just a database
- Not built for authentication/authorization
- No session
- No single sign-on
- Simple attributes
- Simple groups (three different standard mechanisms)

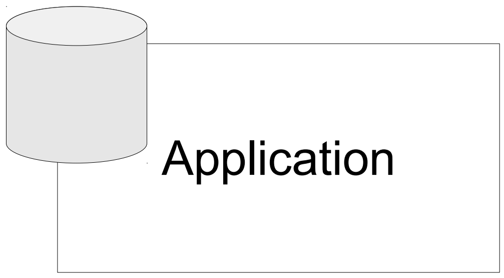
Data Duplication

Data duplication seems to be inevitable

(at least in practical deployments)

- Legacy systems, too expensive to fix
- You just cannot make `join` of relational table and LDAP

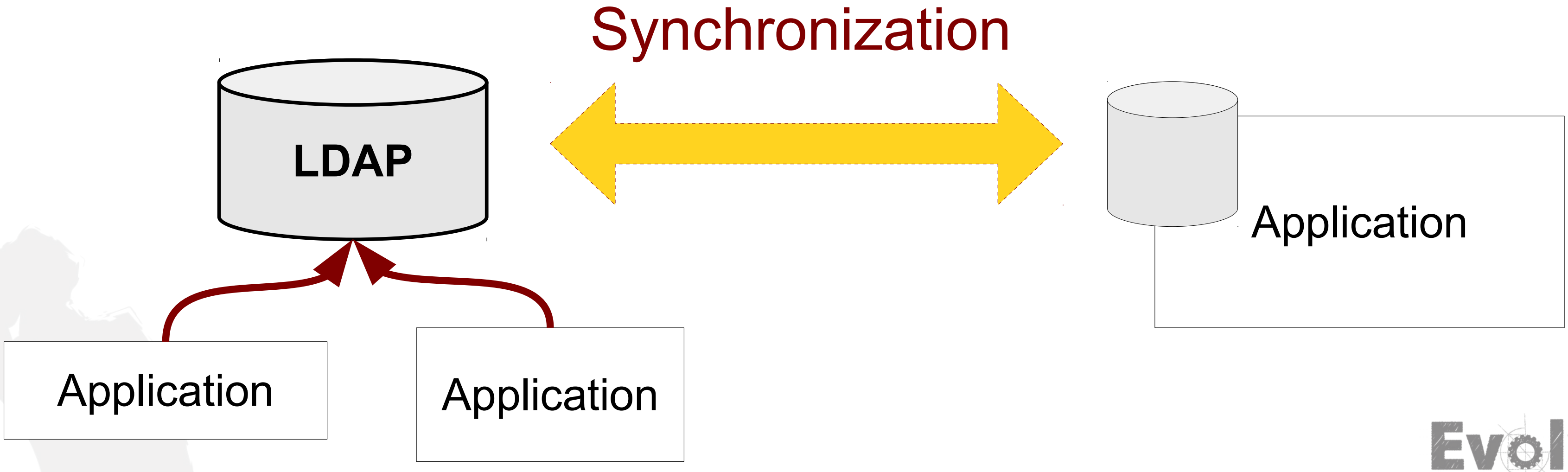




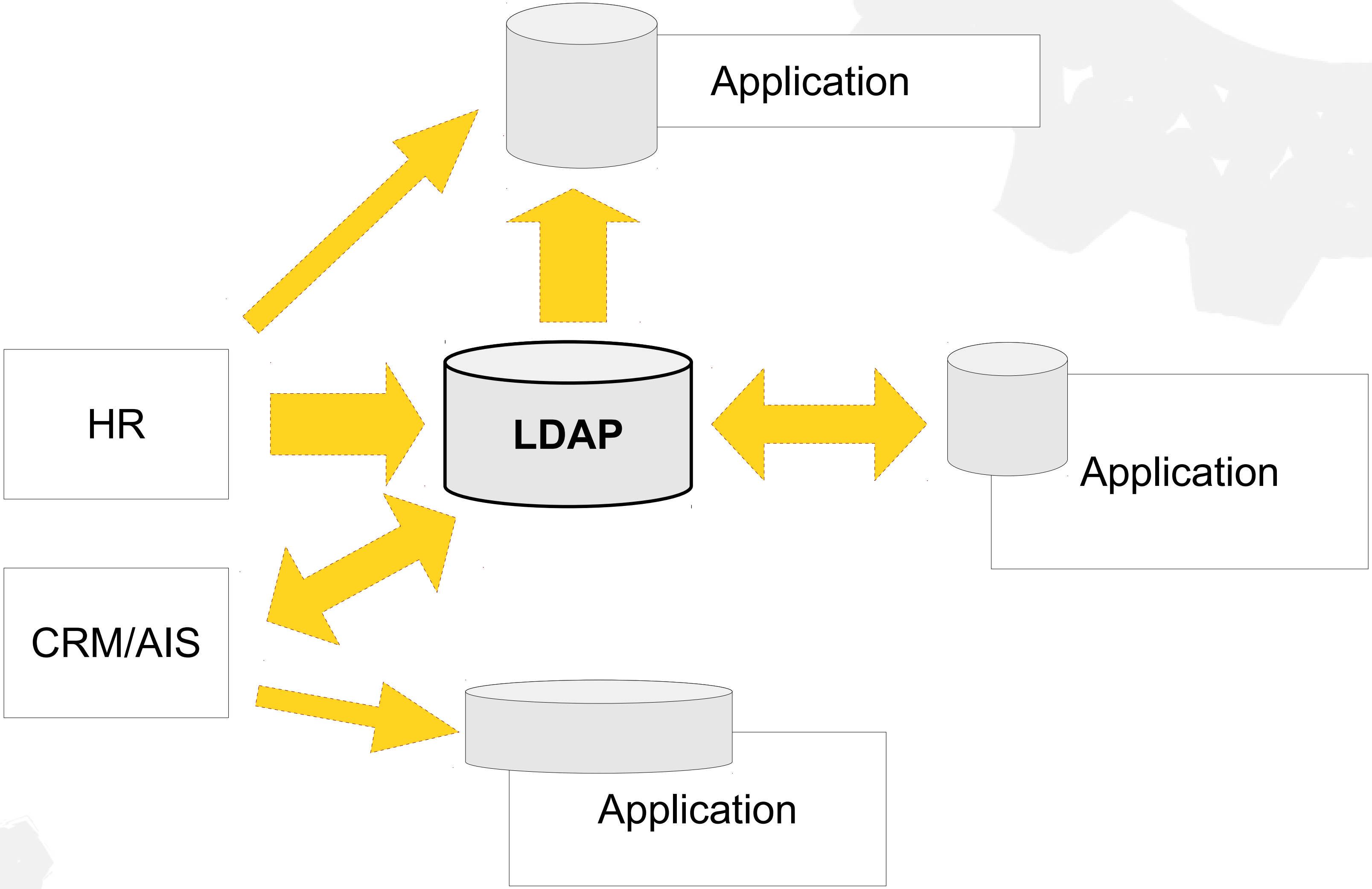
Duplication => Synchronization

How to keep the data consistent?

- Copy data from system to system
- It is (much) harder than it seems



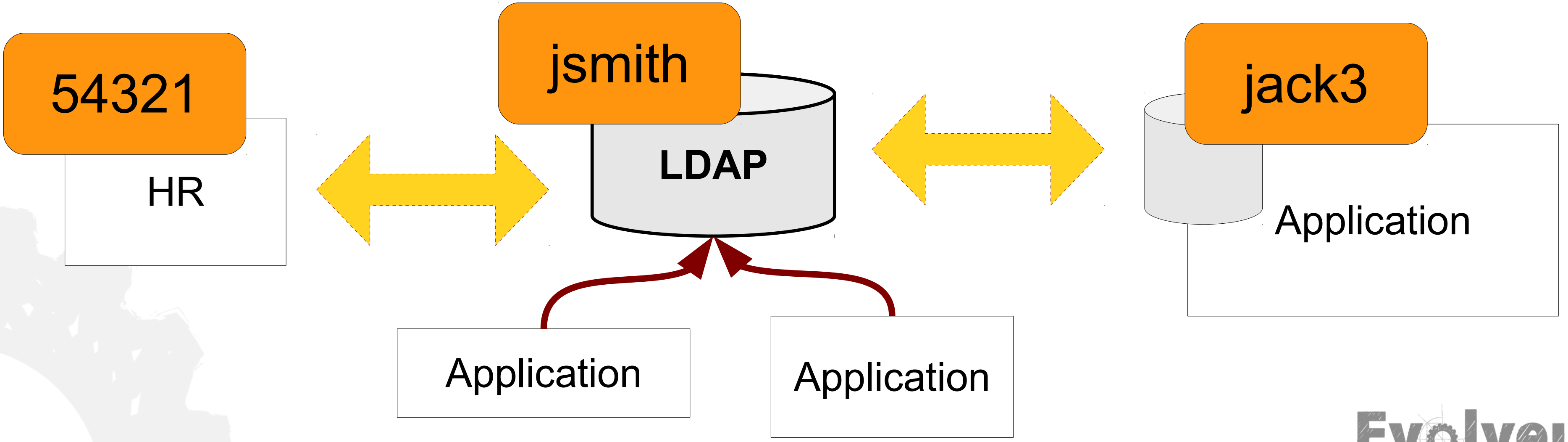
Multi-directional Synchronization



Evolveum

Inconsistent Data

- History (inconsistent identifier assignment)
- Naming constraints (e.g. max 8 chars username)
- Convenience (nobody likes username `x654637ab`)



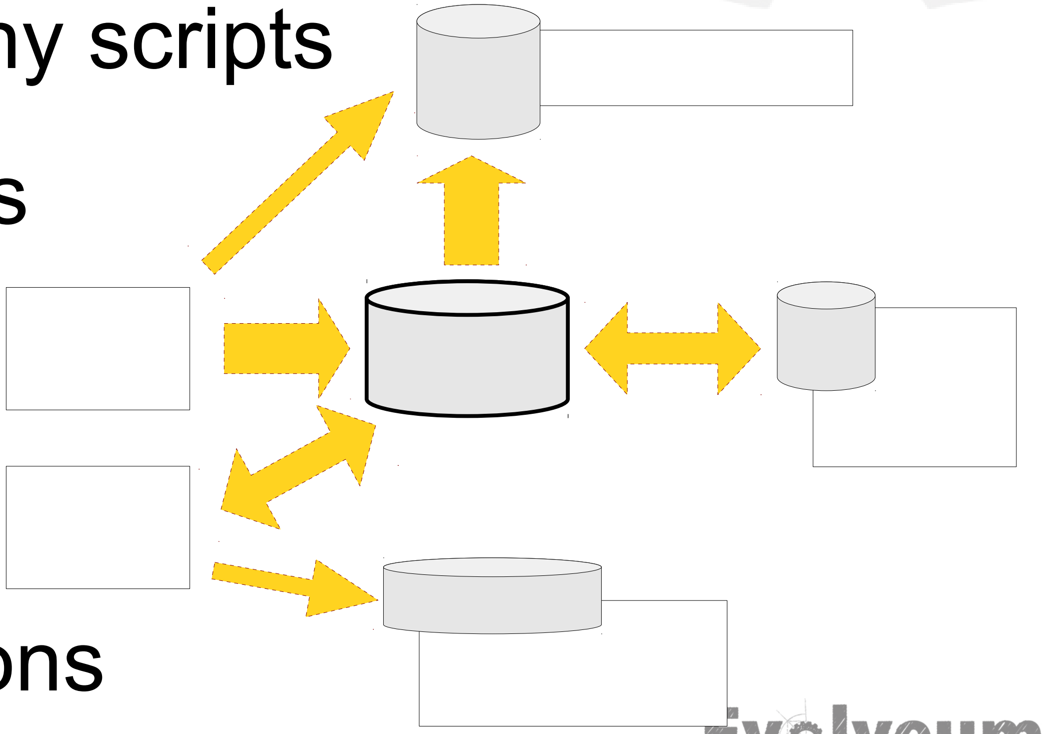
Evolveum

Scripts won't work

Synchronization scripts are easy to create …

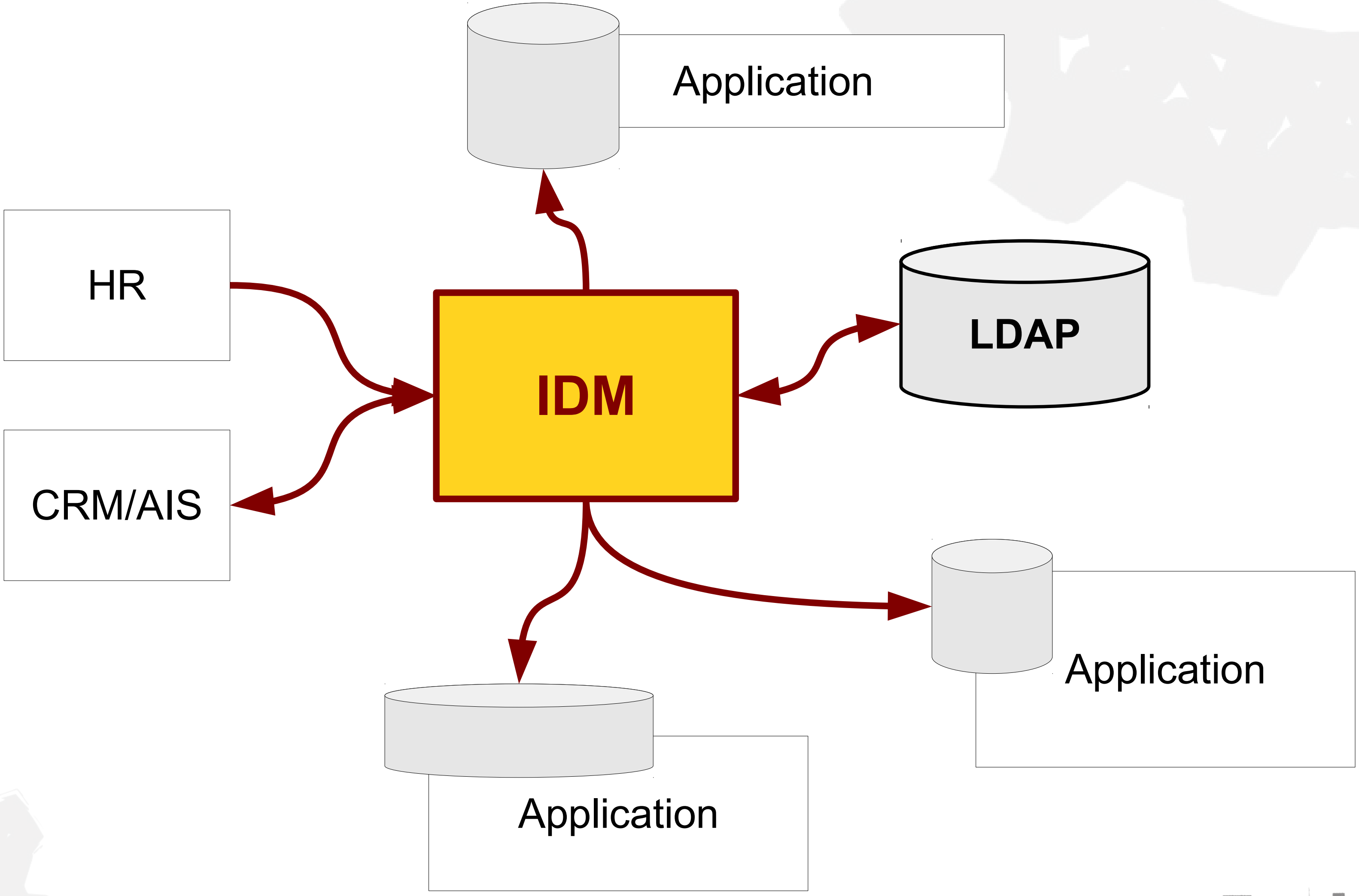
… but very hard to maintain

- Error handling (timeout, retry)
- Many systems = many scripts
- Both directions, loops
- Compare data
- Correlate data
- Policies and exceptions

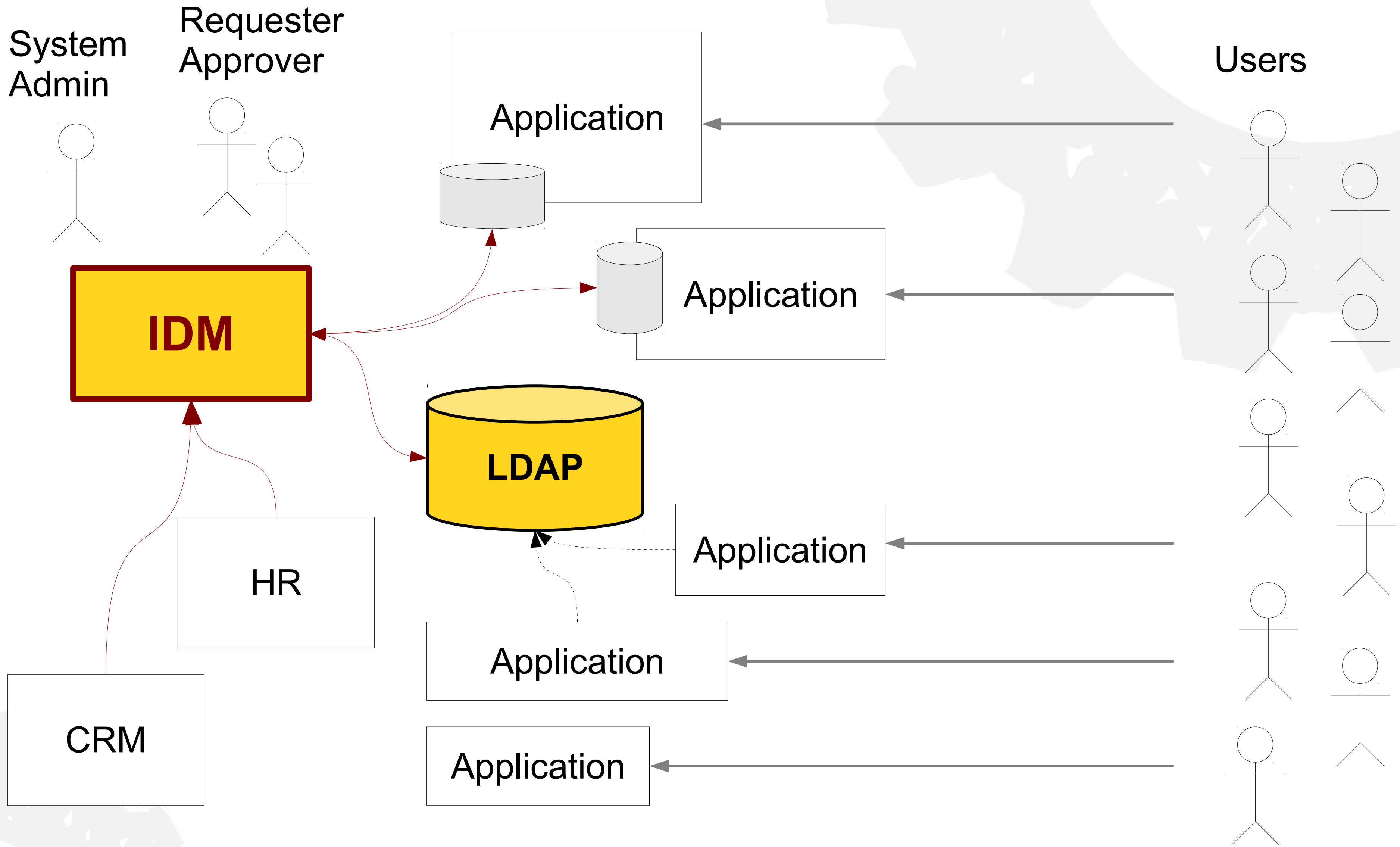


Identity Management

Identity Management (Identity Provisioning)

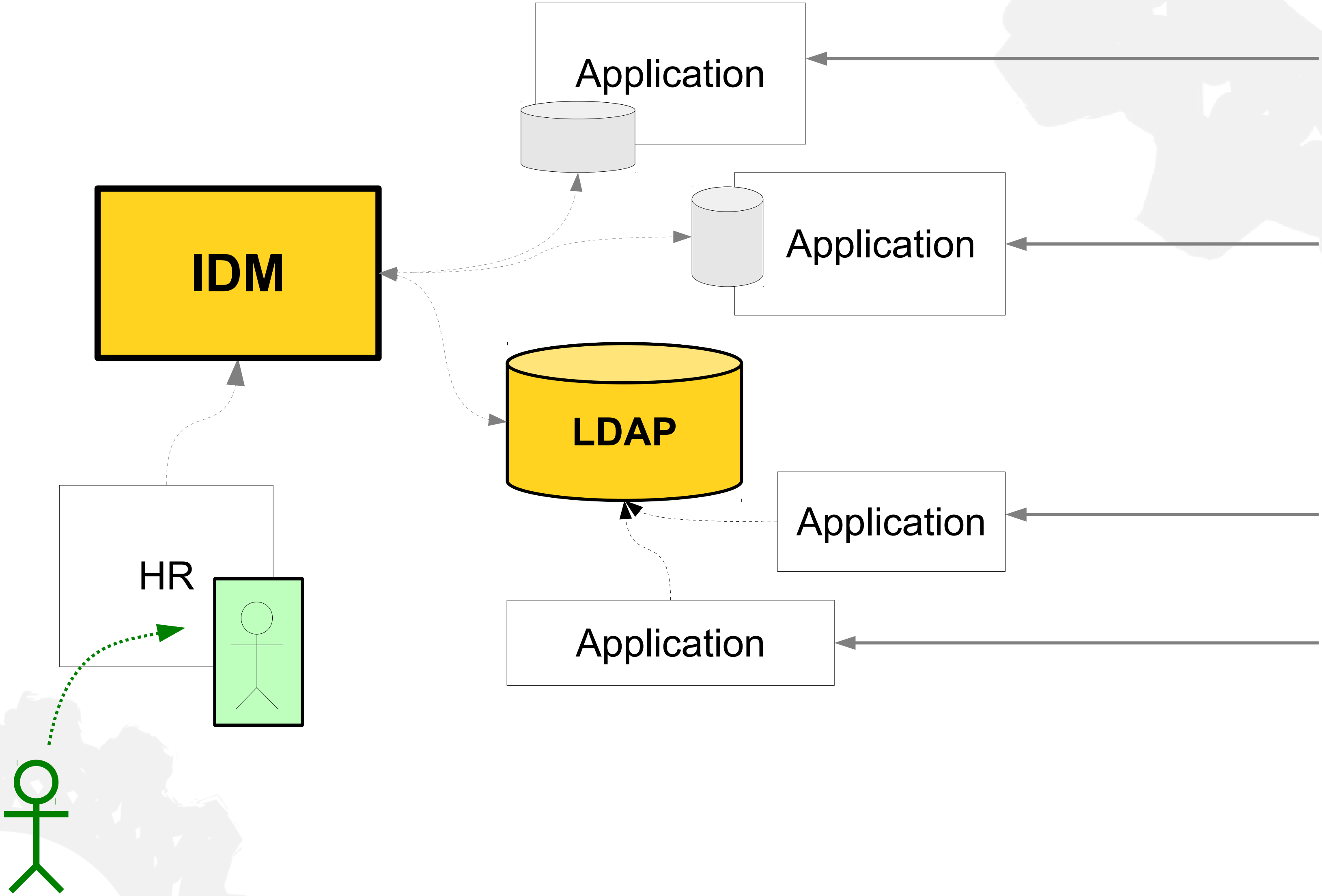


Identity Management

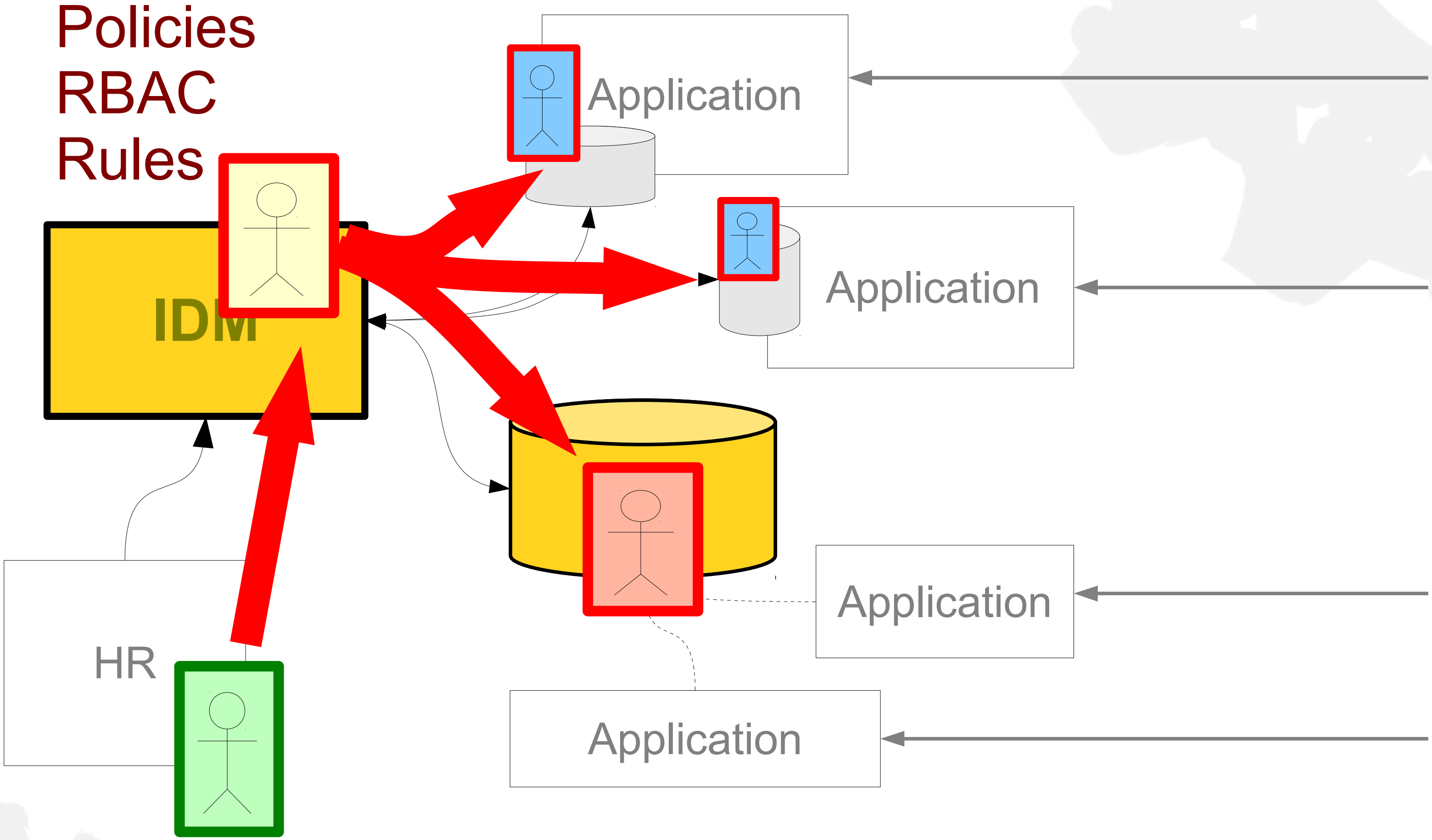


Evolveum

How it works?


Application
Application
IDM
LDAP
Application
HR
Application

Automatic user provisioning

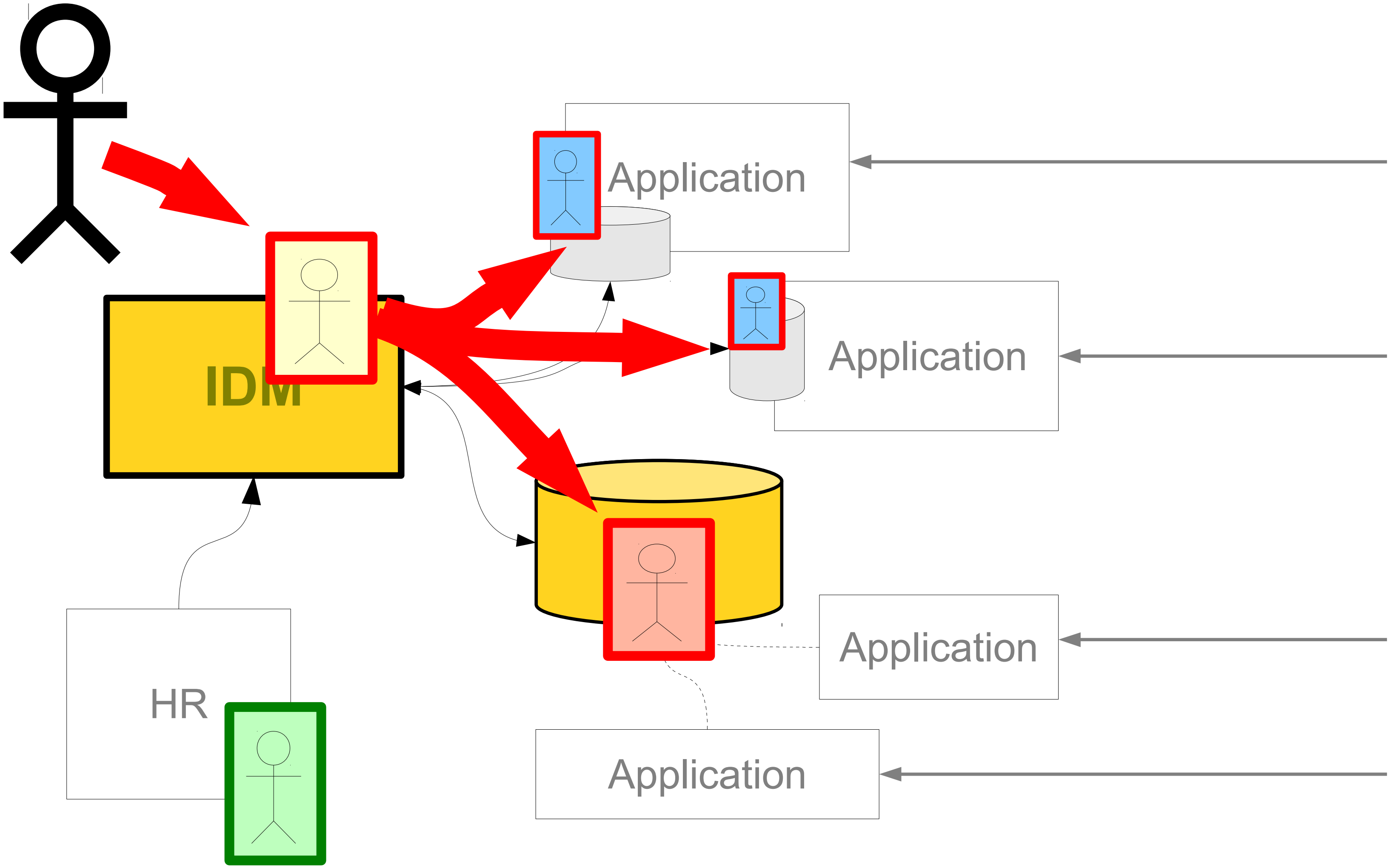


Evolveum

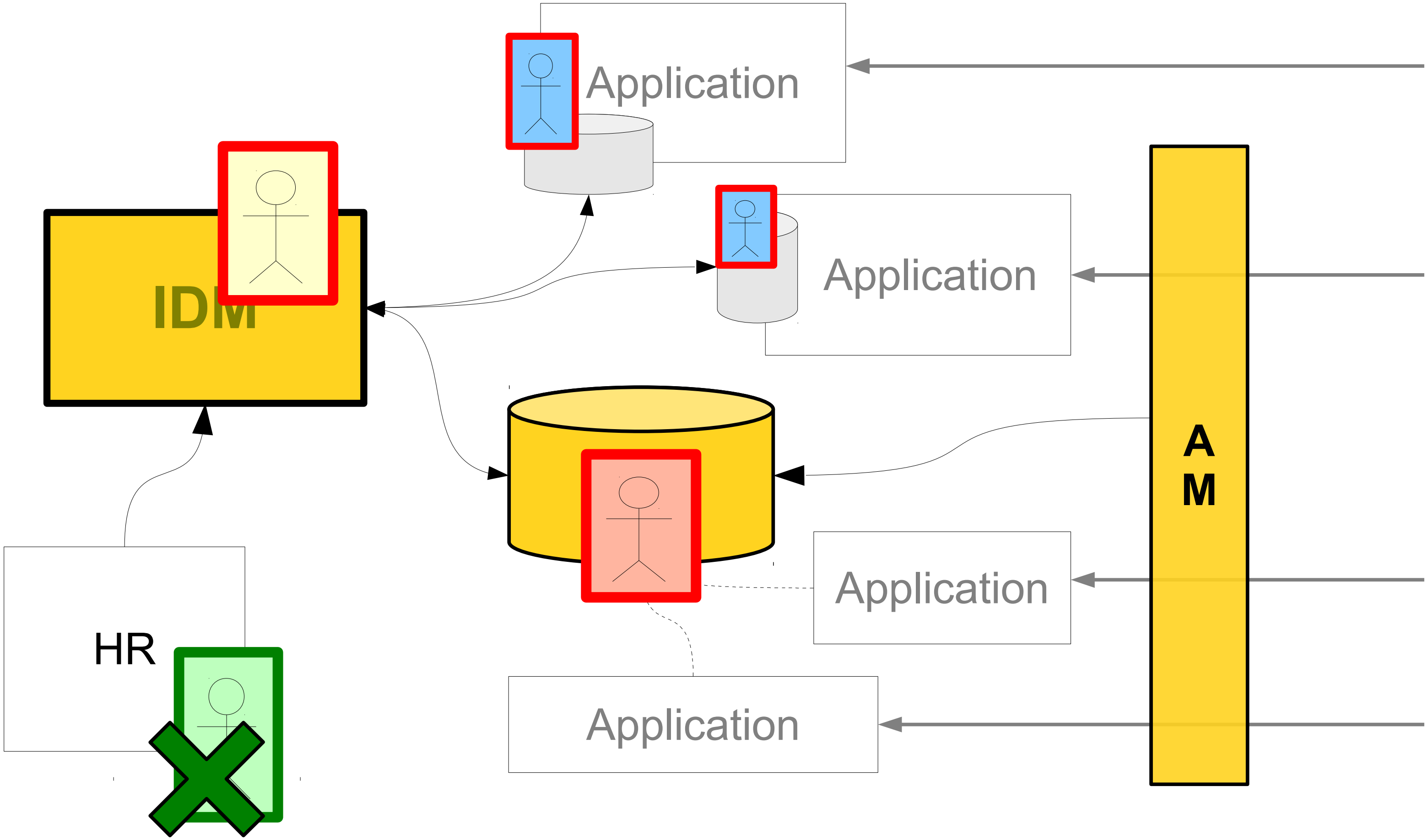
IDM is Much More

- Provisioning, deprovisioning, synchronization
- Role-Based Access Control (RBAC)
- Audit
- Password management
- Workflow: request and approval
- Organizational structure
- Delegated Administration
- ...

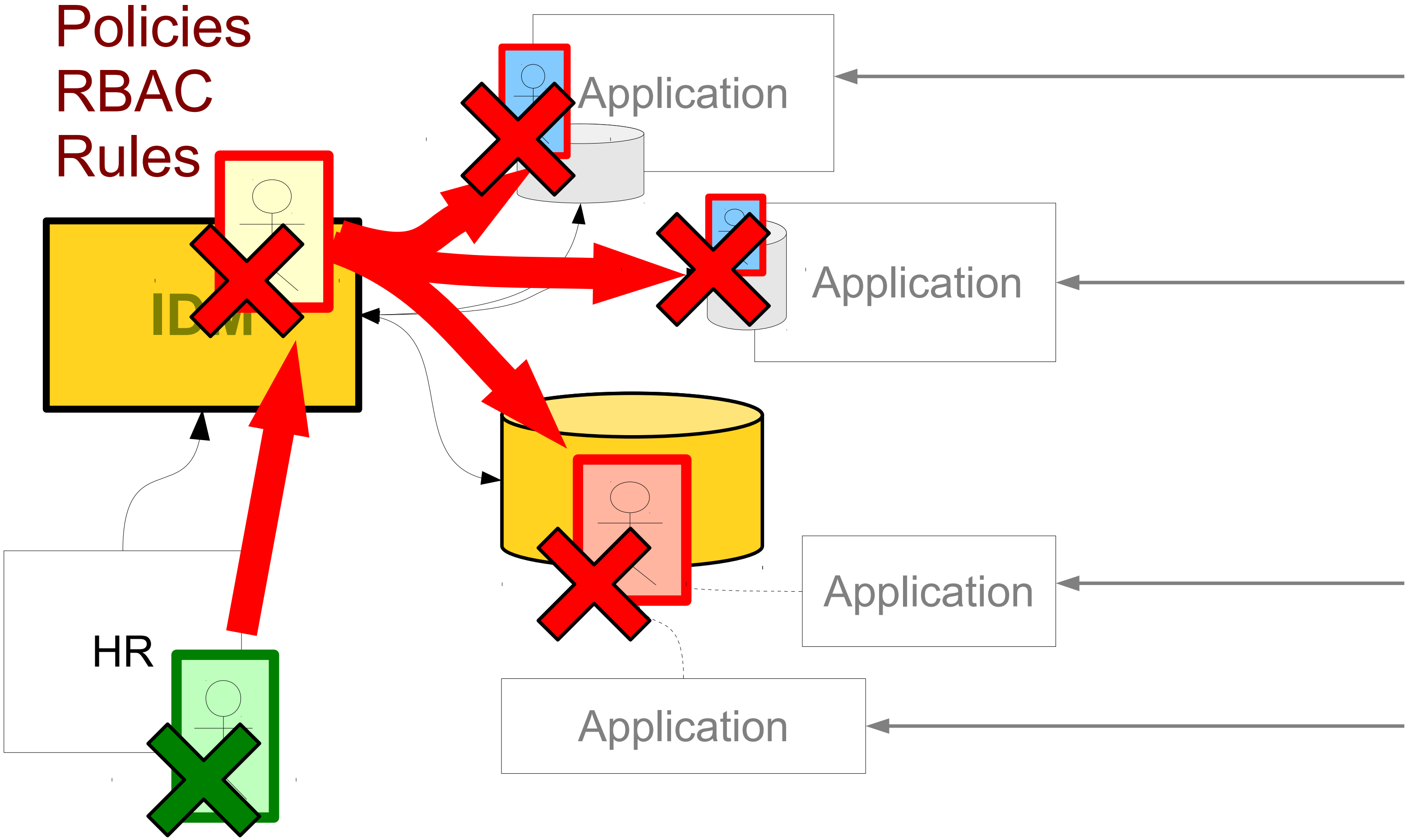
Password reset



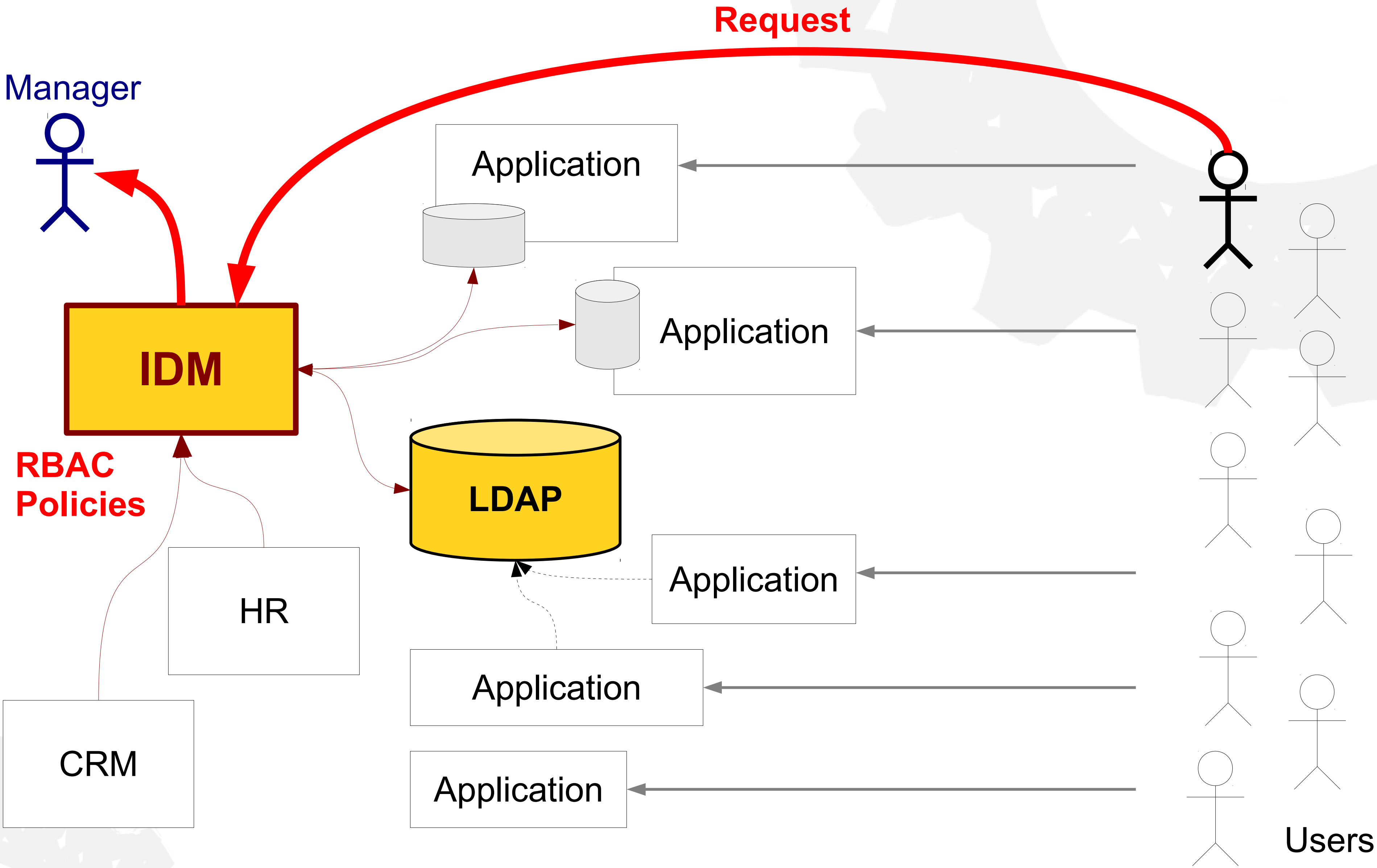
Employee Leaves Company



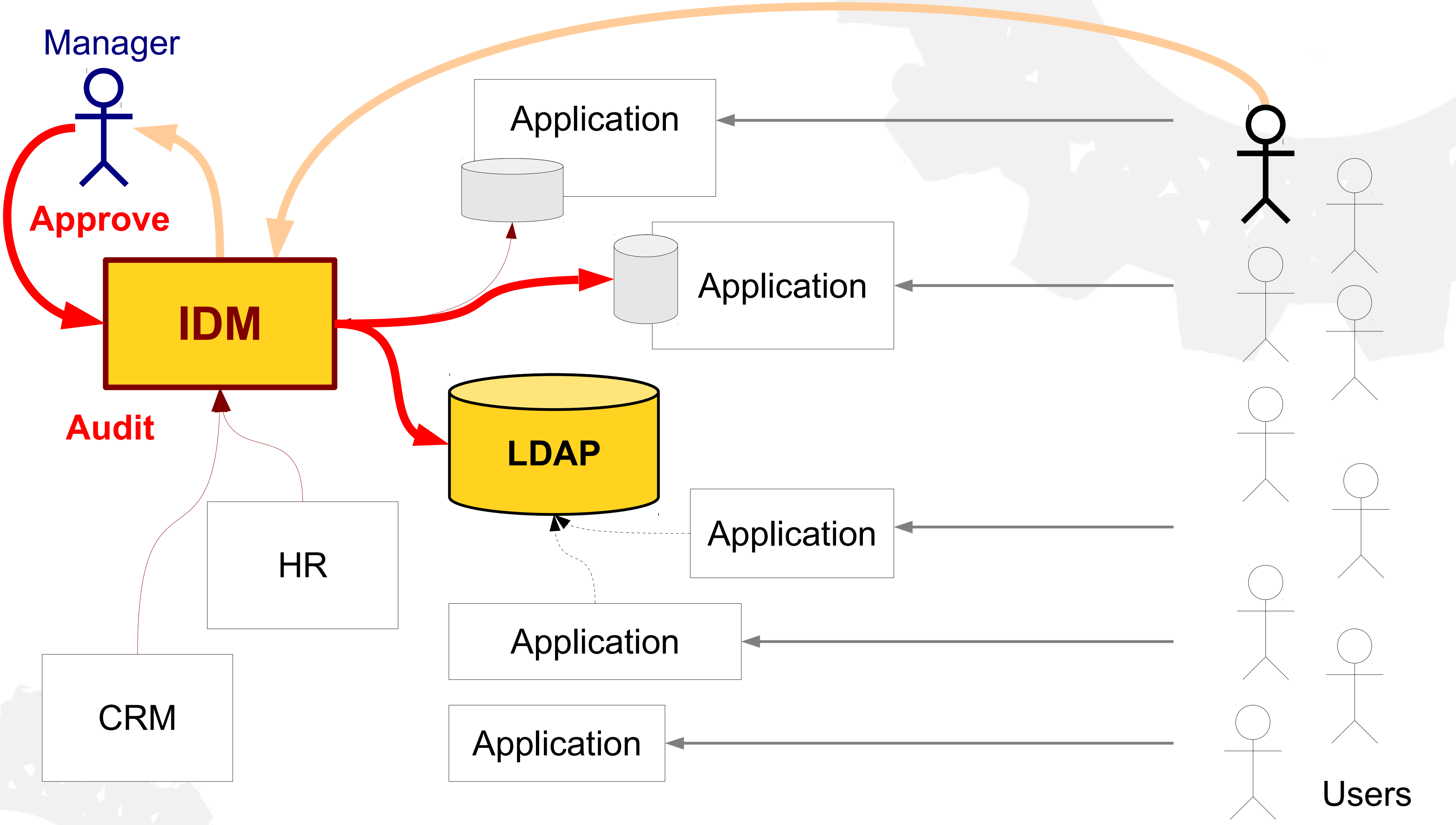
Automatic user deprovisioning



Workflow

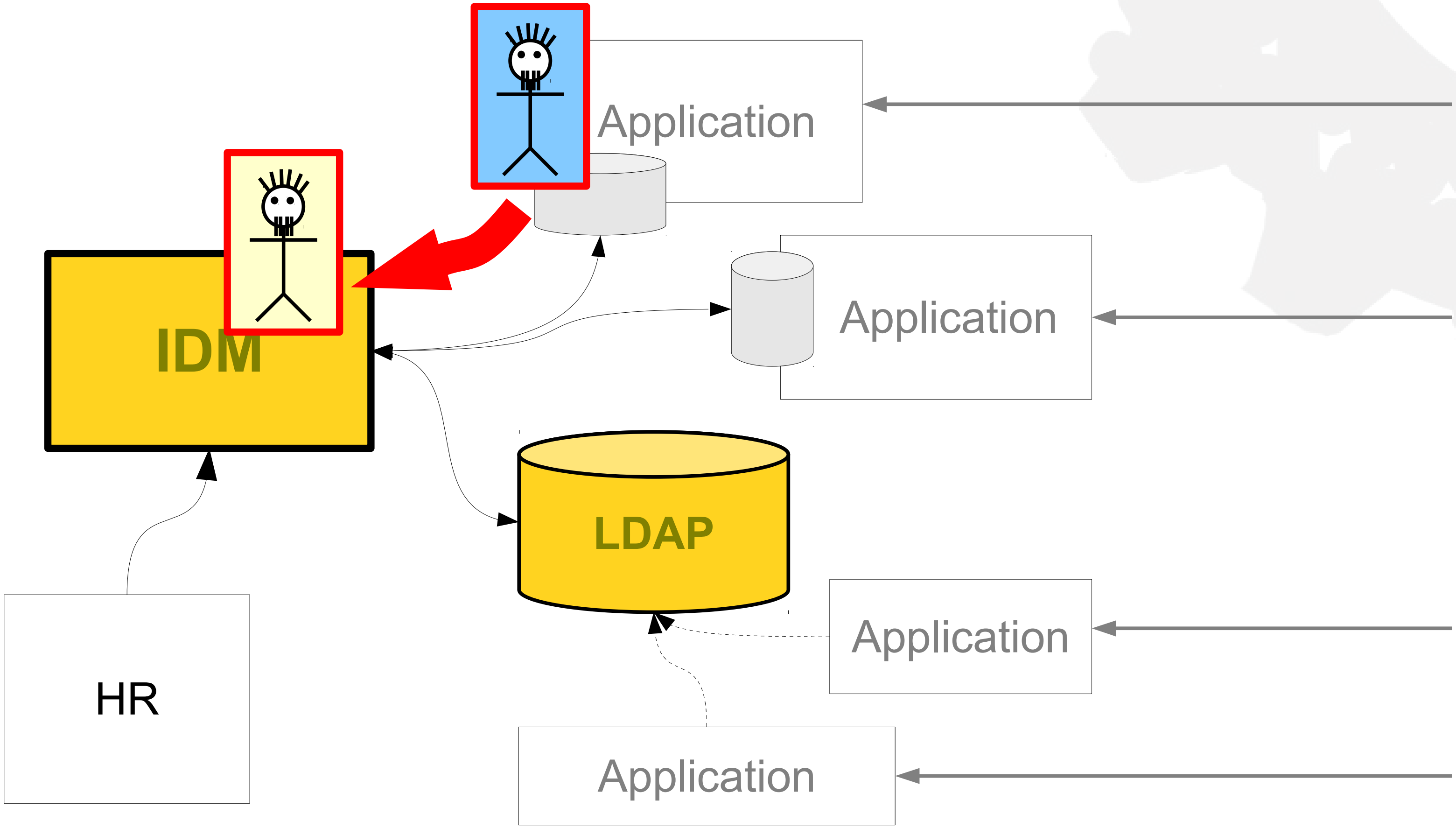

Request
Manager
Application
Application
IDM
RBAC
Policies
LDAP
Application
HR
Application
CRM
Application
Users

Workflow



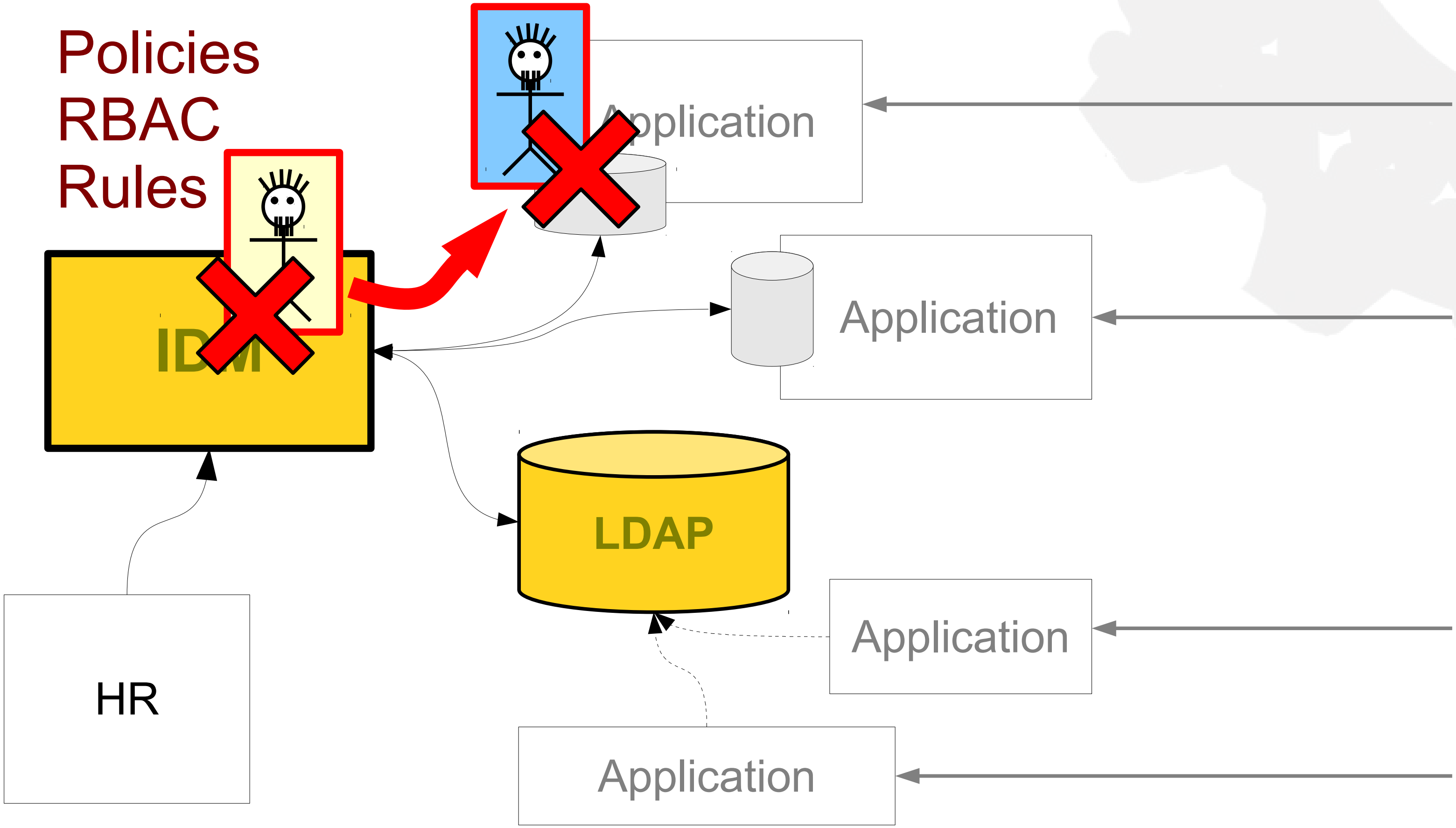
Evolveum

Bidirectional Synchronization



Evolveum

Policy enforcement



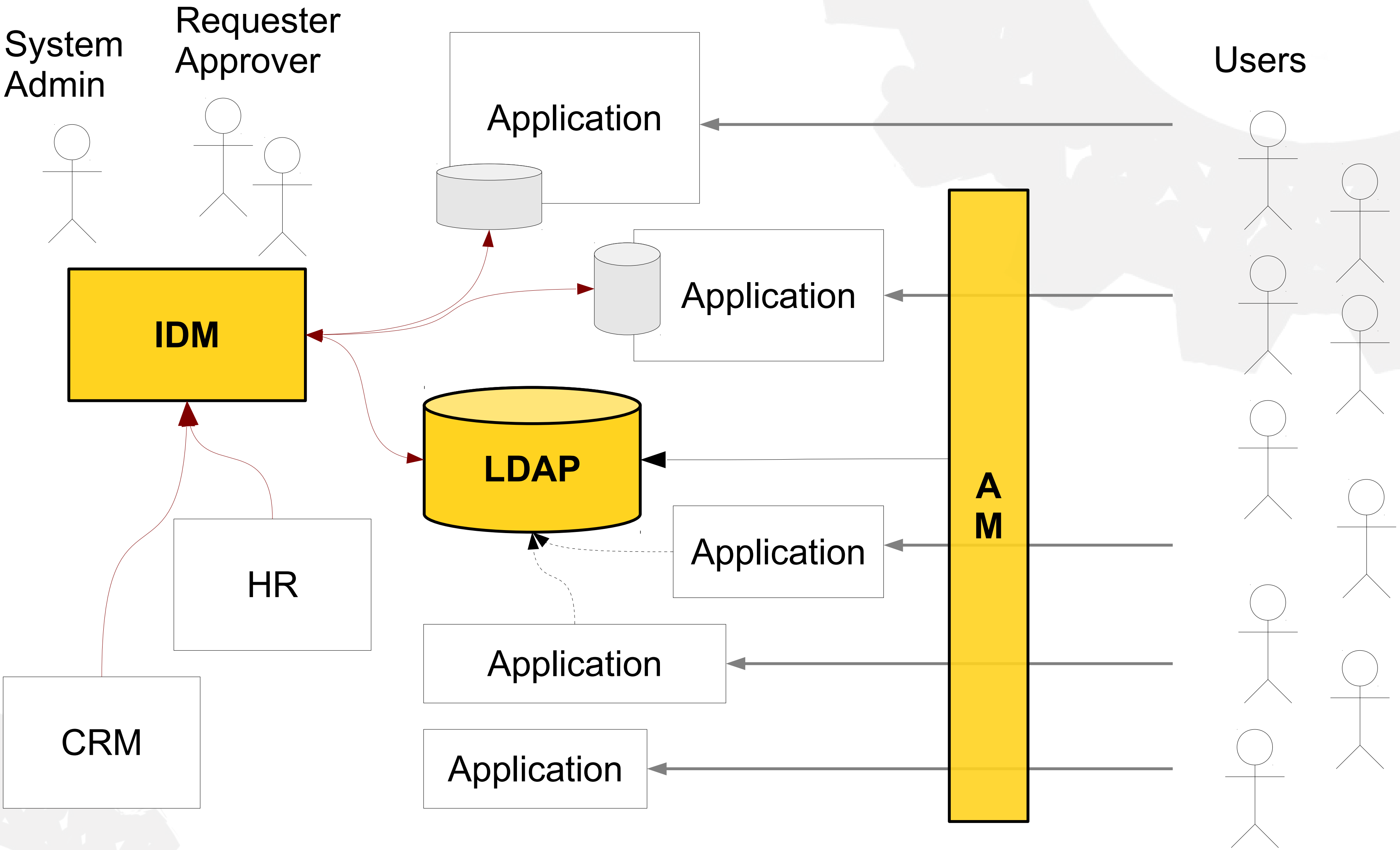
IDM is the First

If you are starting IAM project start with IDM

- IDM will help you clean up the data
- IDM will maintain order
- IDM will enforce policies
- IDM will speed up processes
- IDM for audit and compliance

Access Management

Identity and Access Management



Evolveum

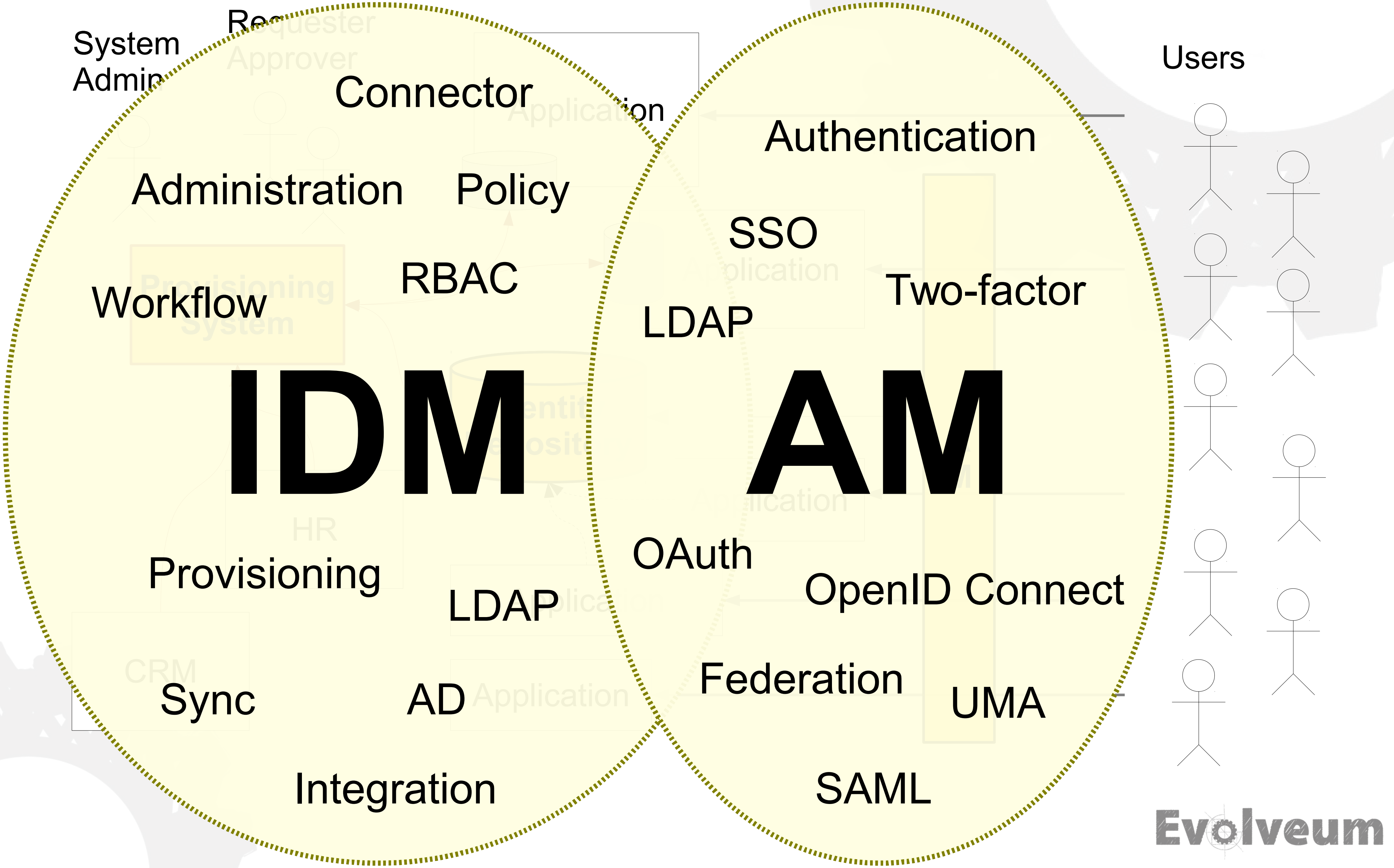
Access Management

- Single Sign-On
- Cross-Domain Single Sign-On
- Federation
- Social login

It needs clean and unified user database

therefore you need IDM first

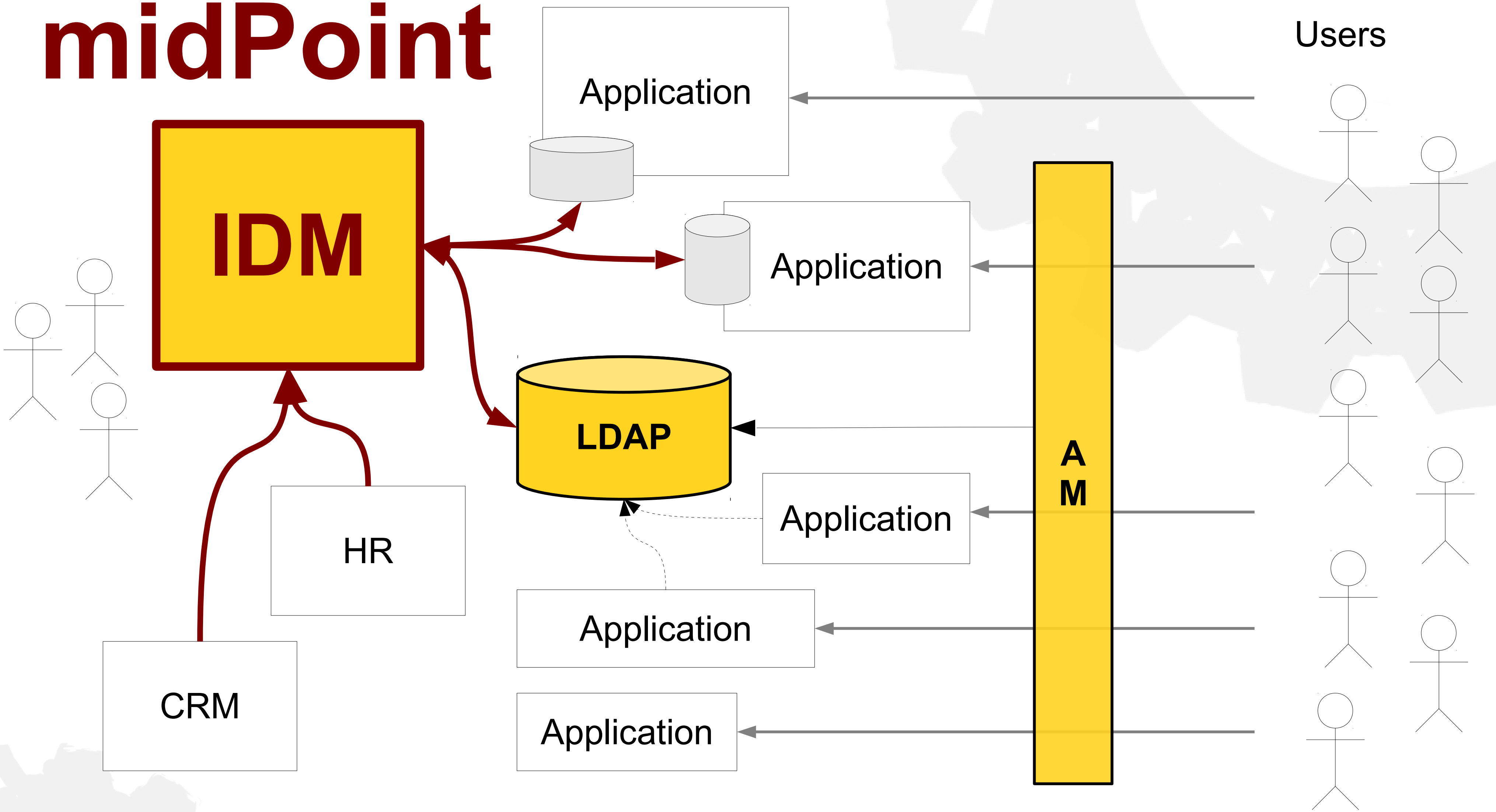
Identity and Access Management



Evolveum

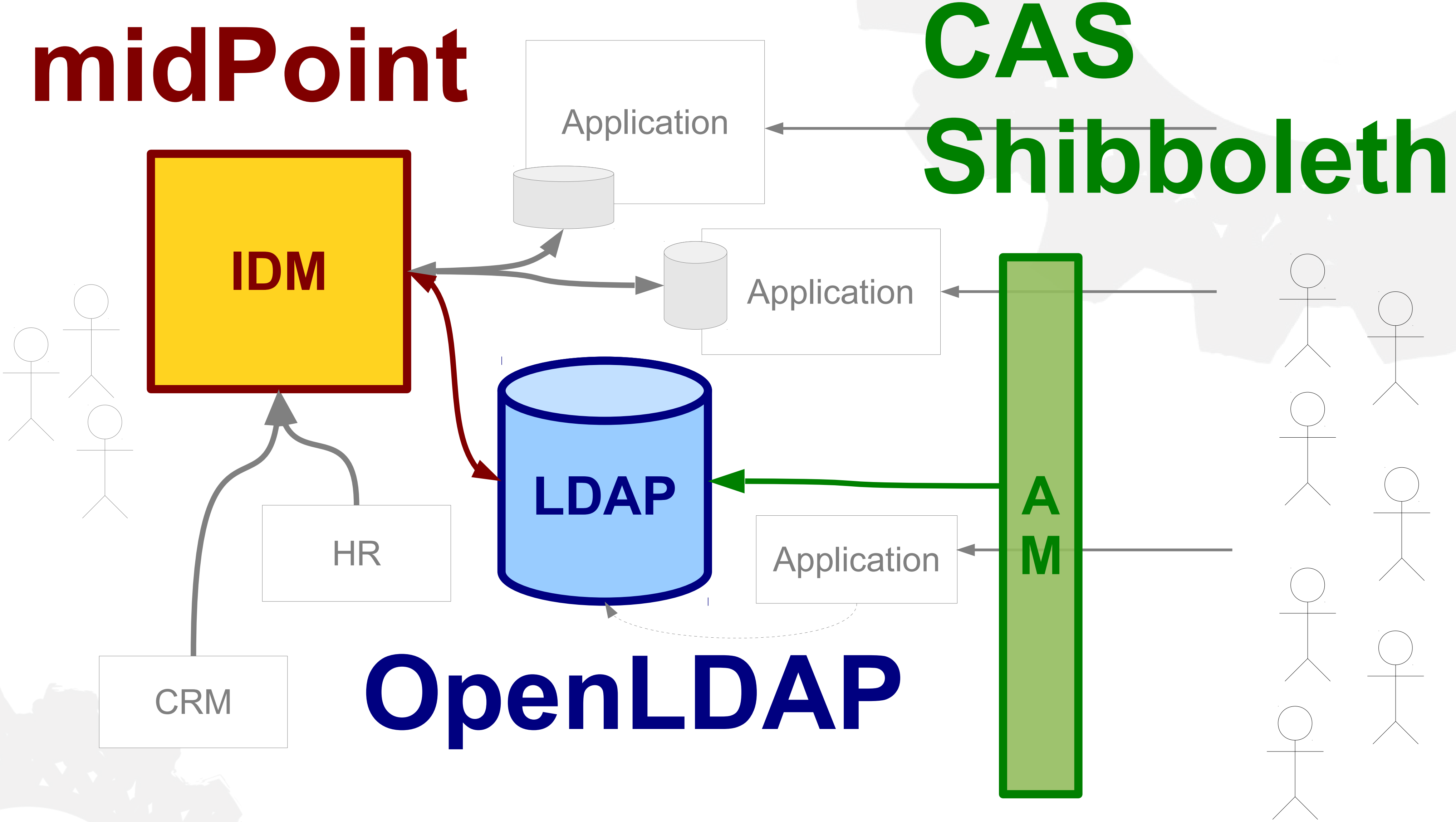
What about Evolveum?

midPoint



Evolveum

100% Open Source Solution



midPoint

CAS
Shibboleth

OpenLDAP

Evolveum

Evolveum

Open Source

Identity Management

Cooperation

Evolveum

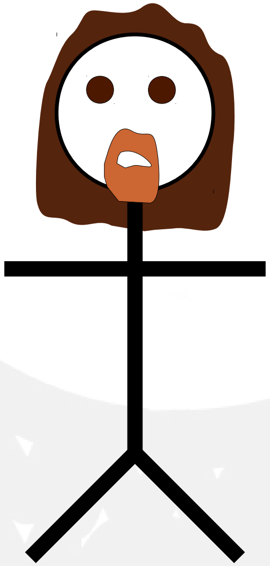
Conclusion

Conclusion

- Identity and Access Management
  - Goal: Operational efficiency & security (audit)
  - Easy to start, complex to maintain
- Identity Management is the start
- midPoint
  - Professional open source provisioning system
  - Next generation system: new technologies and unique features
  - Customer influence and participation

Questions and Answers

Thank You



Radovan Semančík

www.evolveum.com