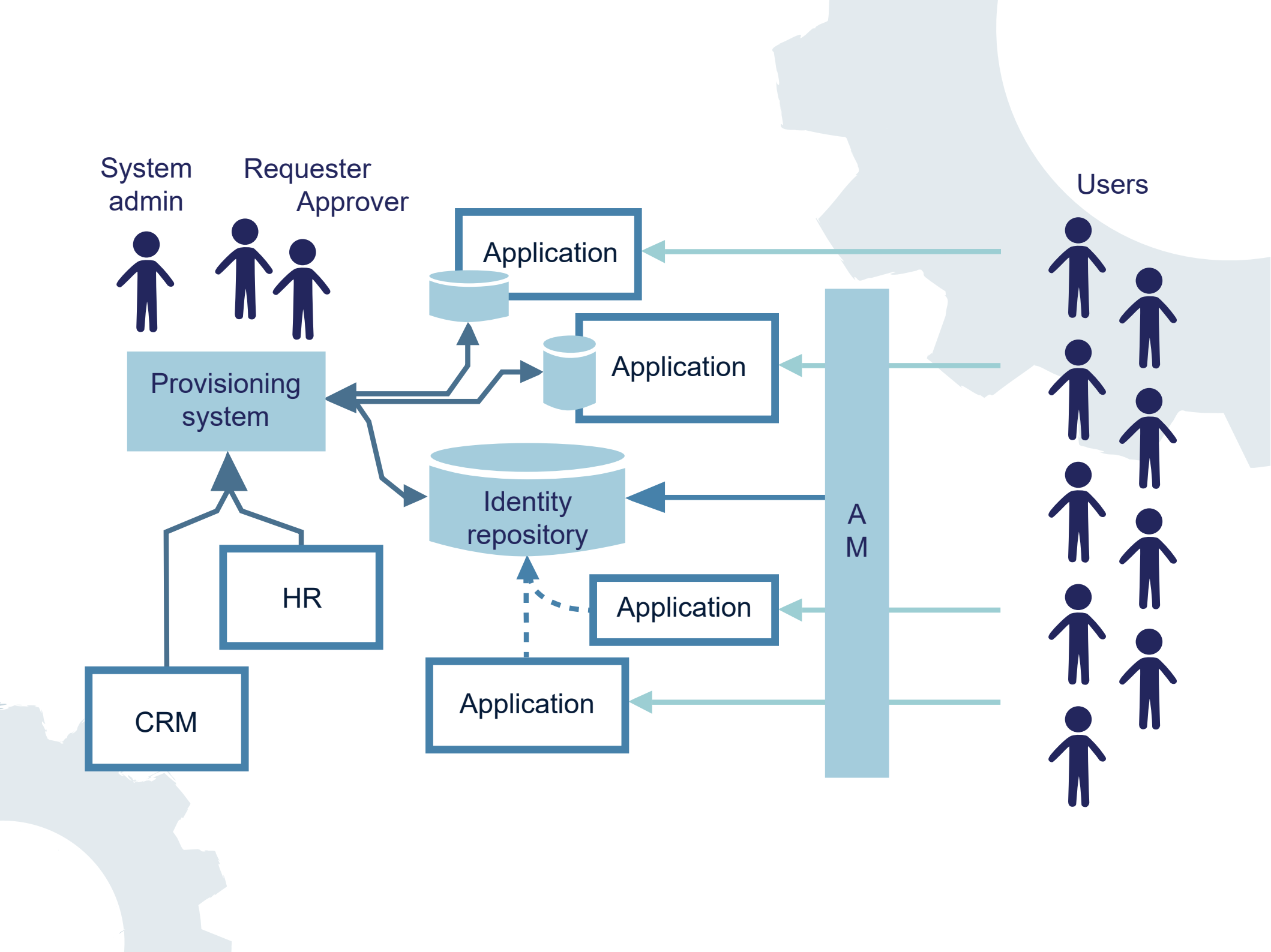
Evolveum

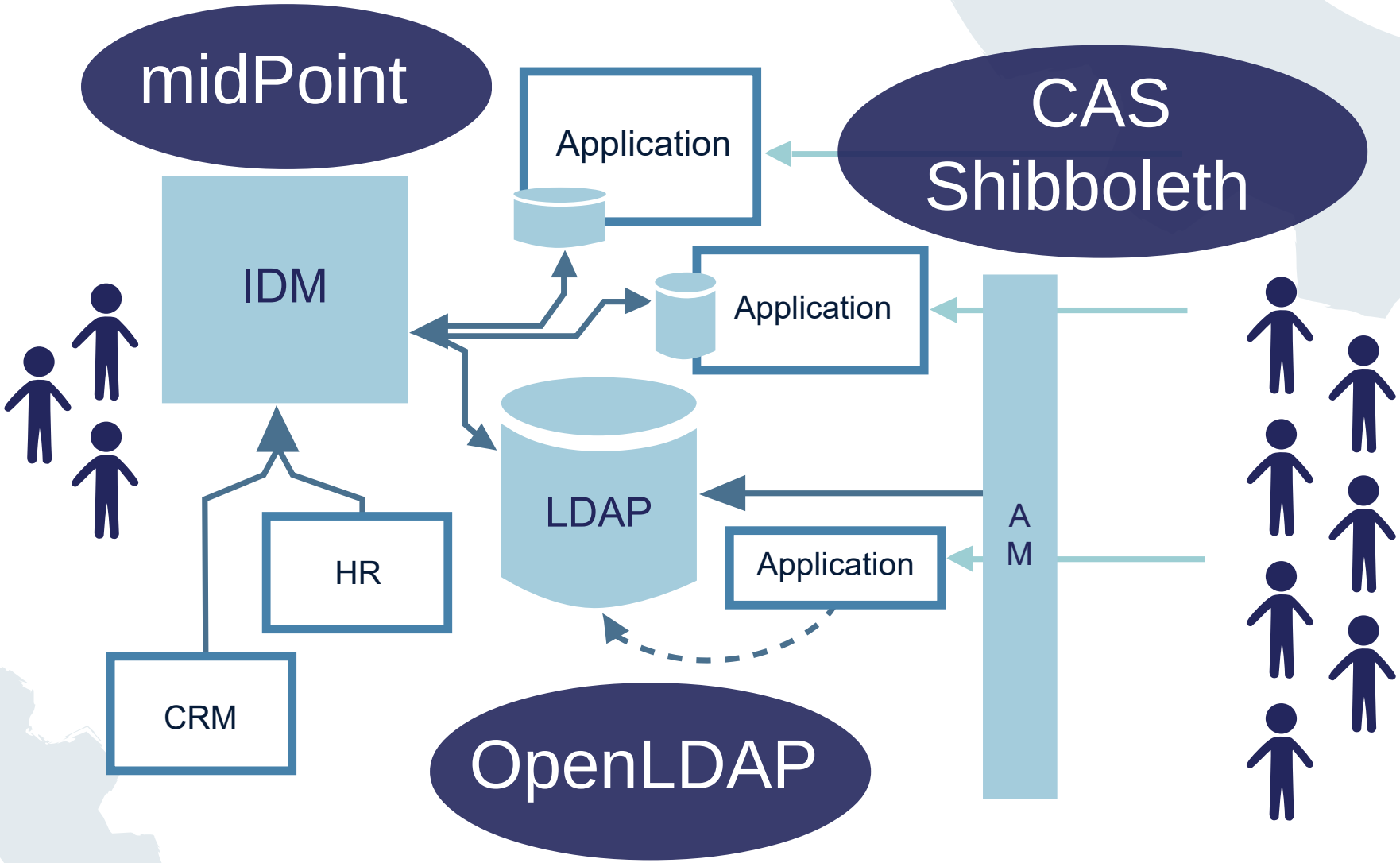
Agenda

- Identity & Access management
- About company
- midPoint
- Clients & partners
- Conclusion

Identity management


System admin
Requester
Approver
Users
Application
Application
Provisioning system
Identity repository
A M
HR
Application
CRM
Application

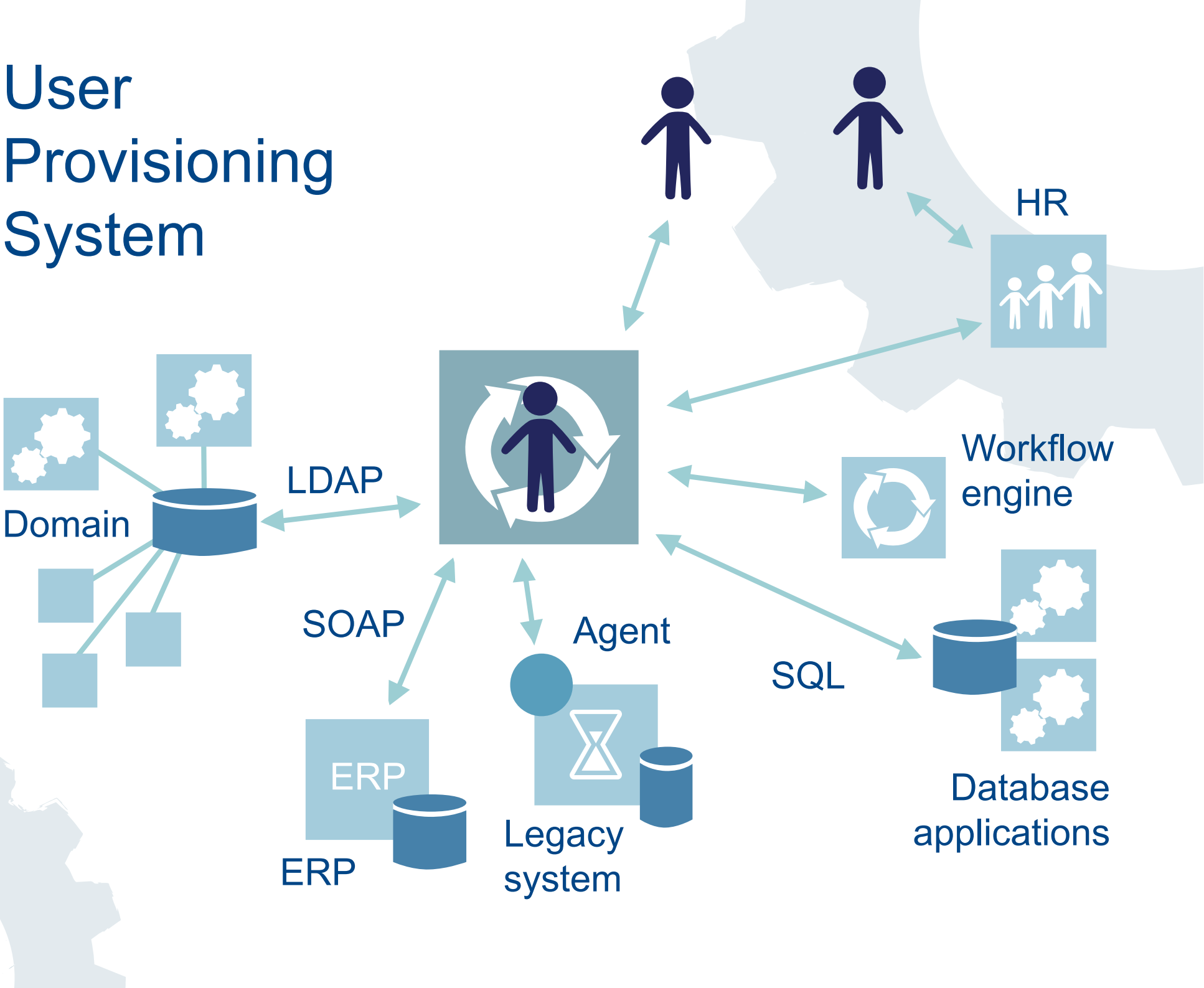
100% Open source solution



Identity management: Provisioning

- Making sure that users have the correct access rights
- Automating the processes of access right management
  - Hiring new employee: creating accounts
  - Reorg: modifications of access privileges
  - Layoffs: deleting/disabling accounts
- Visibility and security
  - Audits, attestations, reporting

User Provisioning System



How does IAM help?

- **Saves money**
  - Cheaper audits, less sysadmin overhead, lower callcenter load
- **Improves efficiency**
  - Faster time to market, minimizes employee wait time
- **Enhances security**
  - Visibility, faster incident responses, cheaper investigation
- **Chaos is reduced**

Identity Management

- Managing user accounts
  - Create, update, delete, rename, password reset, ...
- User self-service
  - Password reset, requesting access, ...
- Driving business processes
  - Approving access requests, ...
- Auditing and Reporting
  - Who and when approved this account?
  - Who's is this **B1gH4x0r** account?

Who can benefit from IAM?

Visibility

Lower cost

Higher workforce efficiency

Time to market

ROI

Cost reduction

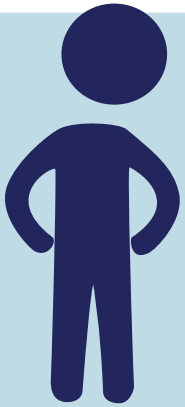
Security

Managers
(Security Officers)

Cost reduction

Much lower workload

Help Desk



TCO reduction

Visibility

Administrators

Higher efficiency

Ability to focus

Visibility

HR

Lower workload

Measurable Benefits (selection)

- Time to get new access rights

  3 weeks → 1 day

- Time to reset a password

  4 hours → 10 minutes

- Call center load reduction

  10-50%

About Evolveum

Evolveum team history

- since approx. 2000
  - various LDAP and IDM projects, various companies
- since 2004: nLight
  - IDM Professional Services
  - Sun Microsystems, Novell
- 2010-2011: Cooperation with ForgeRock
  - Contributing to OpenIDM v1
- 2011: Evolveum
  - Independent development of midPoint
  - Cooperative business model

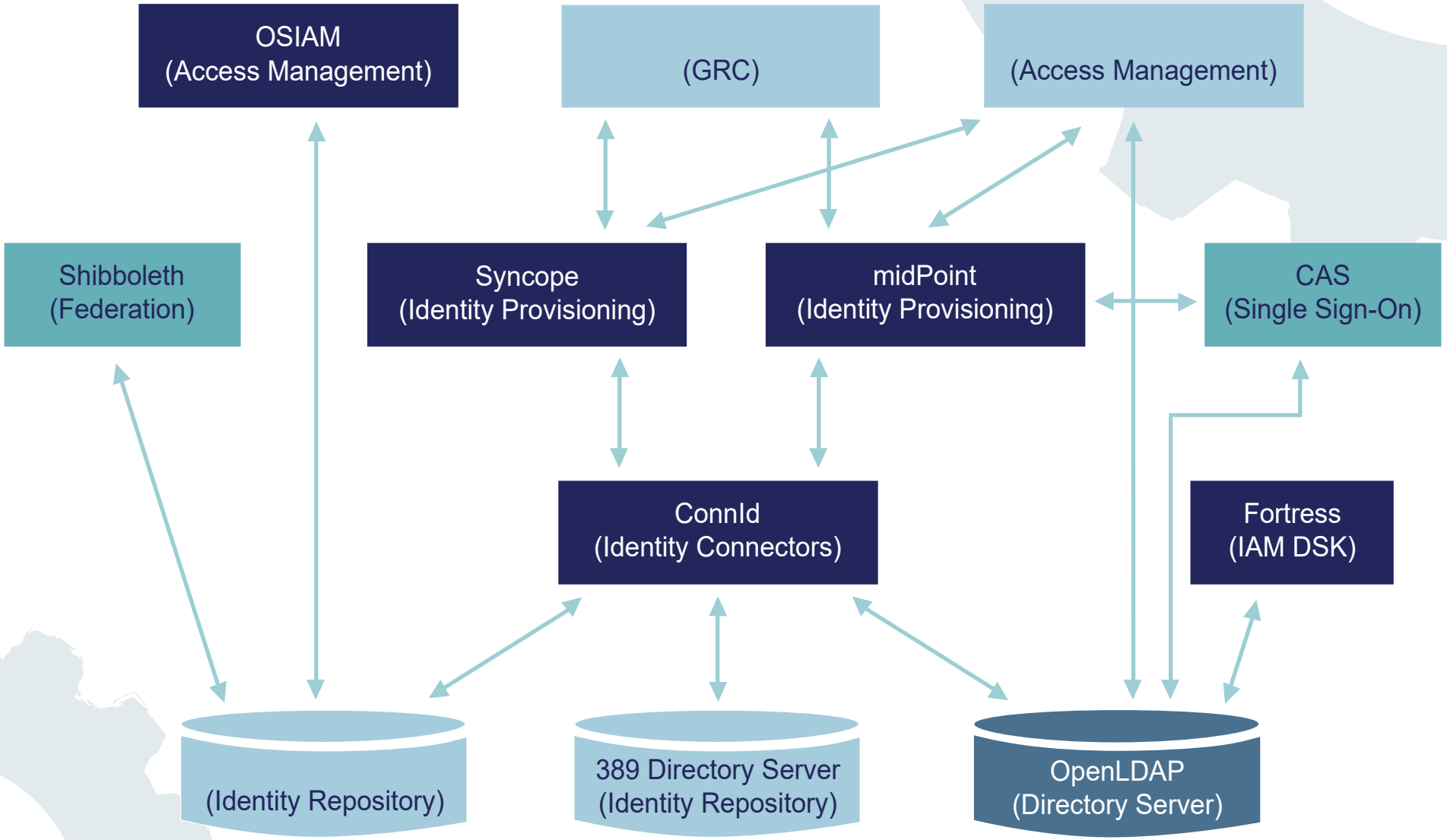
Evolveum

- Focused open source development company
  - Almost all employees are engineers
- Development and research
  - Minimalistic sales and marketing
  - All team members have academic degree (including 2 PhDs)
- Indirect partner-based business
  - Customer – Partner – Evolveum
  - Cooperation is the key

Ecosystem

- Pure open source model
  - No open-core or dual licencing
  - Contributions are welcome
- Distributed development
  - Code created by several development teams
  - Coordinated and integrated by Evolveum
  - Evolveum is a maintainer, not “owner” of the code
- Cooperation instead of domination
  - Evolveum partners add value
    - Cloud, integrated solutions, managed services, extensions, plugins, connectors, ...
  - Trade influence for control to get mutual benefits

Open Source Identity Ecosystem

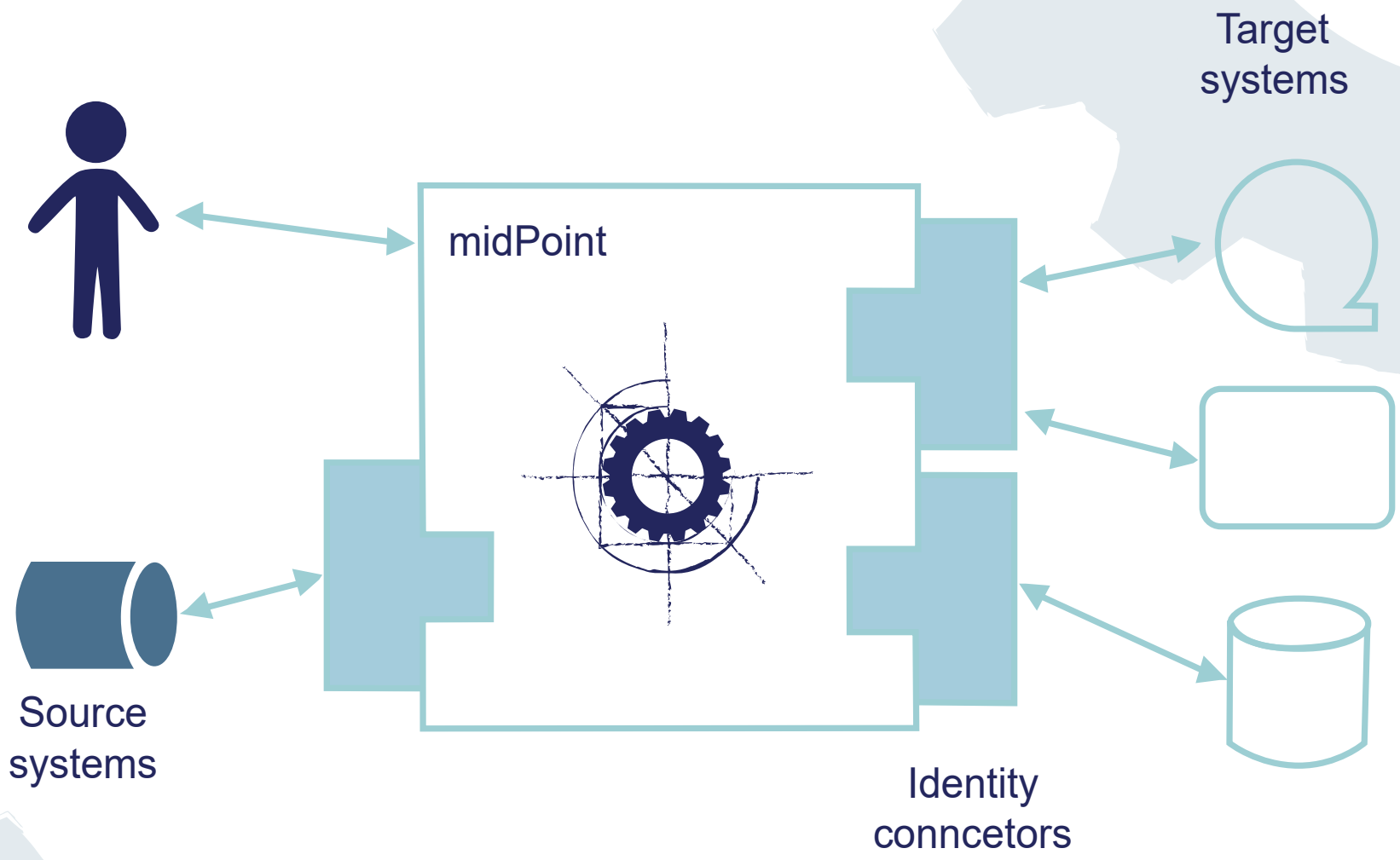


Make the working process smooth by using **OpenSource identity management system**.
Get the work done faster, easier and safe.

MidPoint at glance

- Open-source User Provisioning system
  - 100% open-source, no licence cost, no usage restrictions
- Next-generation system
  - Open architecture, extensible, standard-based, Java/XML/REST
- Deployment and maintenance efficiency
  - 20% of effort to get 80% of result
- Based on a decade of IDM experience

MidPoint big picture



midPoint consists of several parts

- MidPoint core: contains the IDM logic. It is the place where the sophisticated identity management algorithms and policies are implemented.
- Identity connectors: the integration “drivers” that connect midPoint to source and target systems (resources)
- Administration console: a web-based user interface that can be used to configure and manage midPoint. It can also be used for delegated administration, end-user self-service, workflow (approvals), etc.

Unique features

- Advanced RBAC: support of hierarchical, conditional or parametric roles
- Flexible organizational structure support: can model almost any organizational structure as long as it is a acyclic oriented graph.
- Self-healing and resilient system: can automatically heal data inconsistencies whenever they are discovered.
- Generic synchronization: allows to synchronize almost any object, not just users and accounts.
- Adaptivity: if a custom property is added to the user schema then all the other system components automatically adapt.
- Customizable using standardized high-level languages: There are no proprietary languages that lead to vendor lock-in.
- Clean extensible architecture: A proper component-based system decomposition documented using UML diagrams.
- Openness: midPoint is designed, built, developed and maintained entirely in an open fashion. No part of midPoint is closed or kept secret.

midPoint in numbers

- At least 13 years of IDM experience
- At least 11 years of research (12 publications)
- Almost 5 years of active development (10 releases)
- More than 460 000 lines of code
- Estimated project cost: $ 9 837 844 (COCOMO, openhub.net)
- Average 200 commits per month (total 8396 commits)
- More than 3300 automated tests
- Almost 500 wiki pages containing documentation

Past, present and future

midPoint history

- 2004: nLight – IDM specialist company
  - Mostly Sun IDM (but also other technologies)
- 2009: Sun acquired by Oracle
  - Death of Sun IDM ….. end of business?
- Spring 2010: OpenIDMv1
  - nLight cooperating with ForgeRock on OpenIDM development
- Spring 2011: ForgeRock is changing course
  - OpenIDMv2 plan: drop everything, reinvent everything
- May 2011: midPoint project start
  - Evolveum established by nLight and others
  - Based on OpenIDMv1 code created by nLight
- 2012 and on: independent development
  - Still cooperating with ForgeRock (e.g. OpenICF)

Roadmap

- midPoint 2.x RELEASED
  - Basic and some advanced functionality
- MidPoint 3.0 (Newton) RELEASED
  - Delegated administration, generic sync, REST, …
- MidPoint 3.1, 3.1.1 (Sinan) RELEASED
  - Improved GUI, wizards, …
- MidPoint 3.2 (Tycho) RELEASED
  - Recertification, synchronization GUI, …
- MidPoint 3.3 (Lincoln) RELEASED
  - New GUI & SelfService, Binary attributes support, …
- MidPoint 3.4 (Heisenberg) RELEASED
  - GUI usability features and customizations, production ready certifications, ...

Current State (version 3.4)

- Access certification (production quality)
- Entitlement approval support
- Major GUI improvements
- Governance features
- Significant user interface improvements
- LDAP-based AD connector in full production quality
- Matching rule for XML-formatted string attributes and UUIDs
- Full support for Java 8 environment (both build and runtime)
- Improved documentation
- And more

MidPoint 3.x is revolutionary

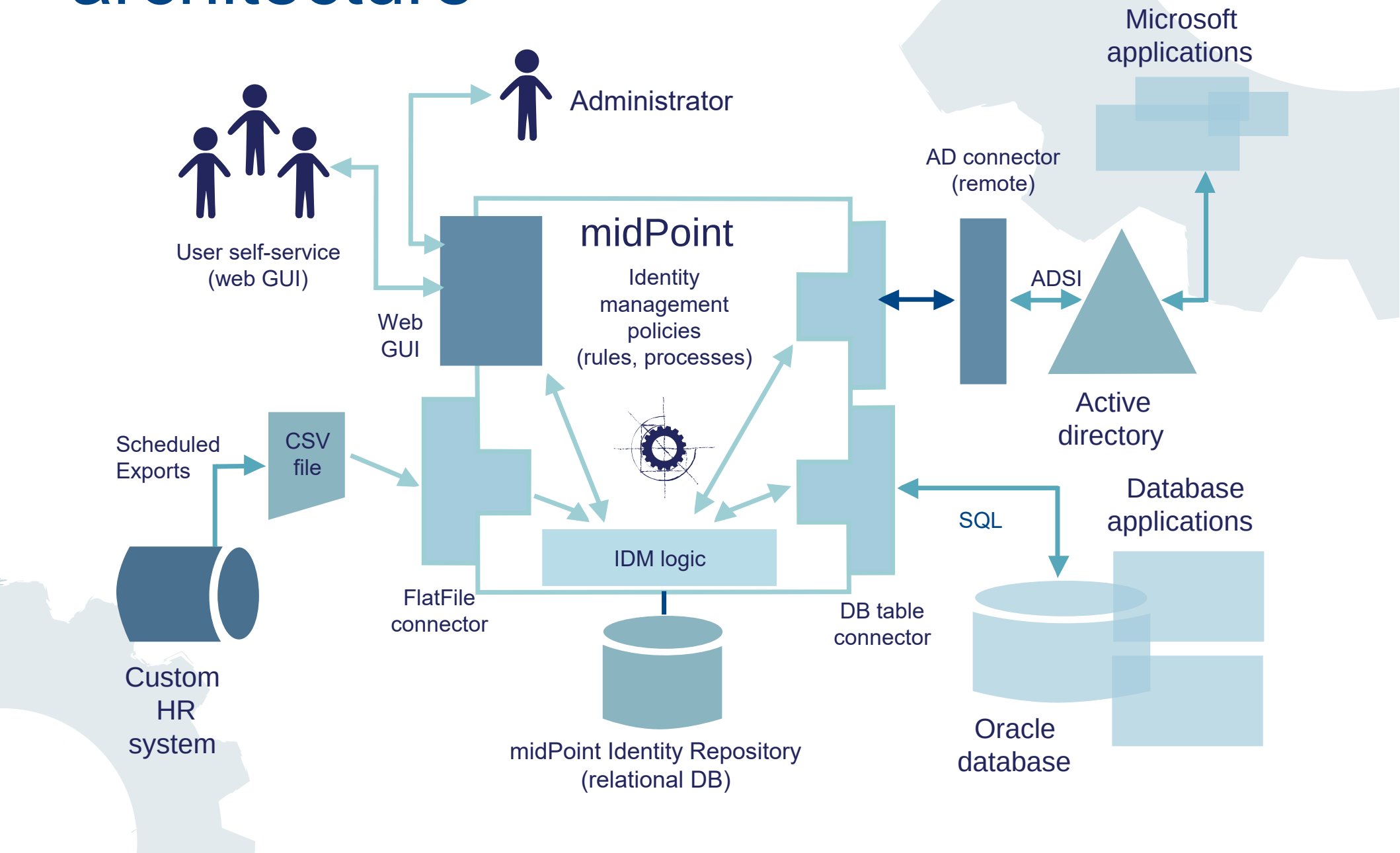
- It goes **beyond** Identity Management
- Generic Synchronization
  - Synchronize everything with everything
- Entitlements
  - Support for groups and privileges (PIM)
- REST (and JSON and YAML later)
- Delegated Administration
  - Fine-grained authorizations + organizational structure
- New GUI Look and Feel - Customizable

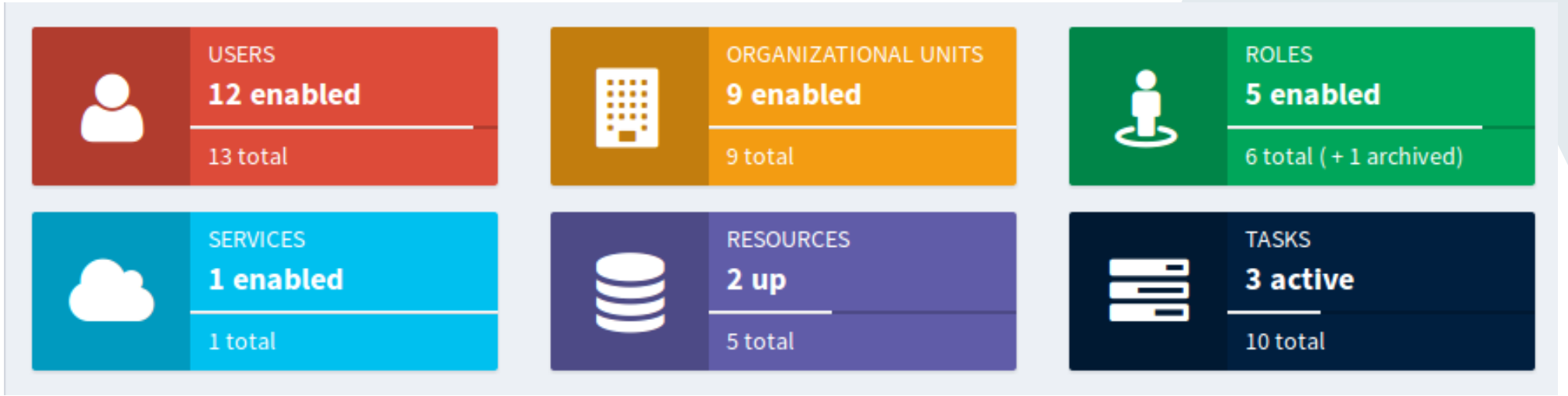
Open and dynamic development

- Completely open development
  - Public distributed source code management (git, planned soon)
  - Public task tracking (Jira)
  - Public communication and documentation (mailing lists, wiki)
  - Public planning (roadmap, Jira)
- User (customer) participation
  - (Paying) customers influence roadmap and take precedence
  - MidPoint users can influence the development plan
- Contributions

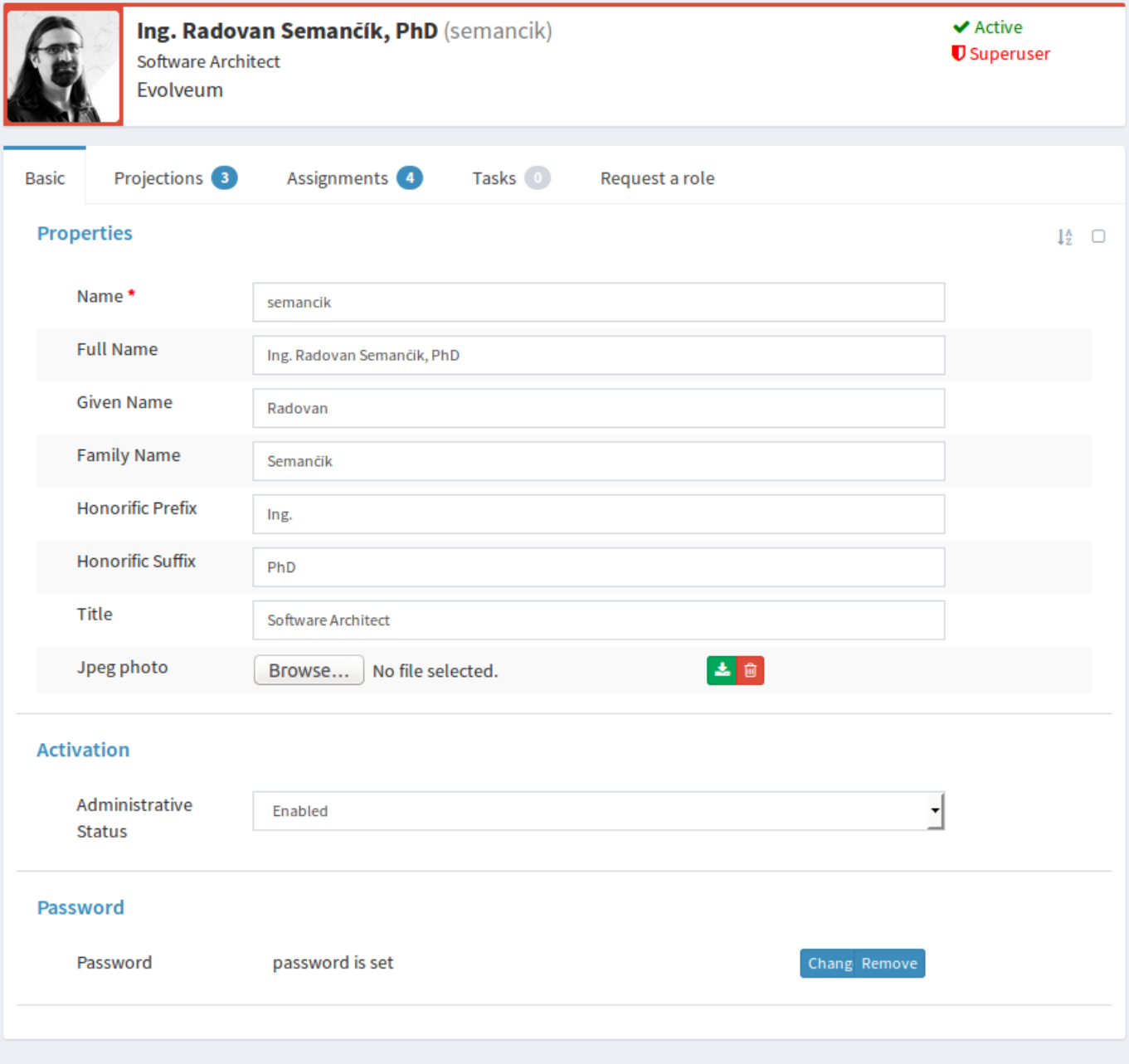
midPoint deployment example

Example of midPoint deployment architecture

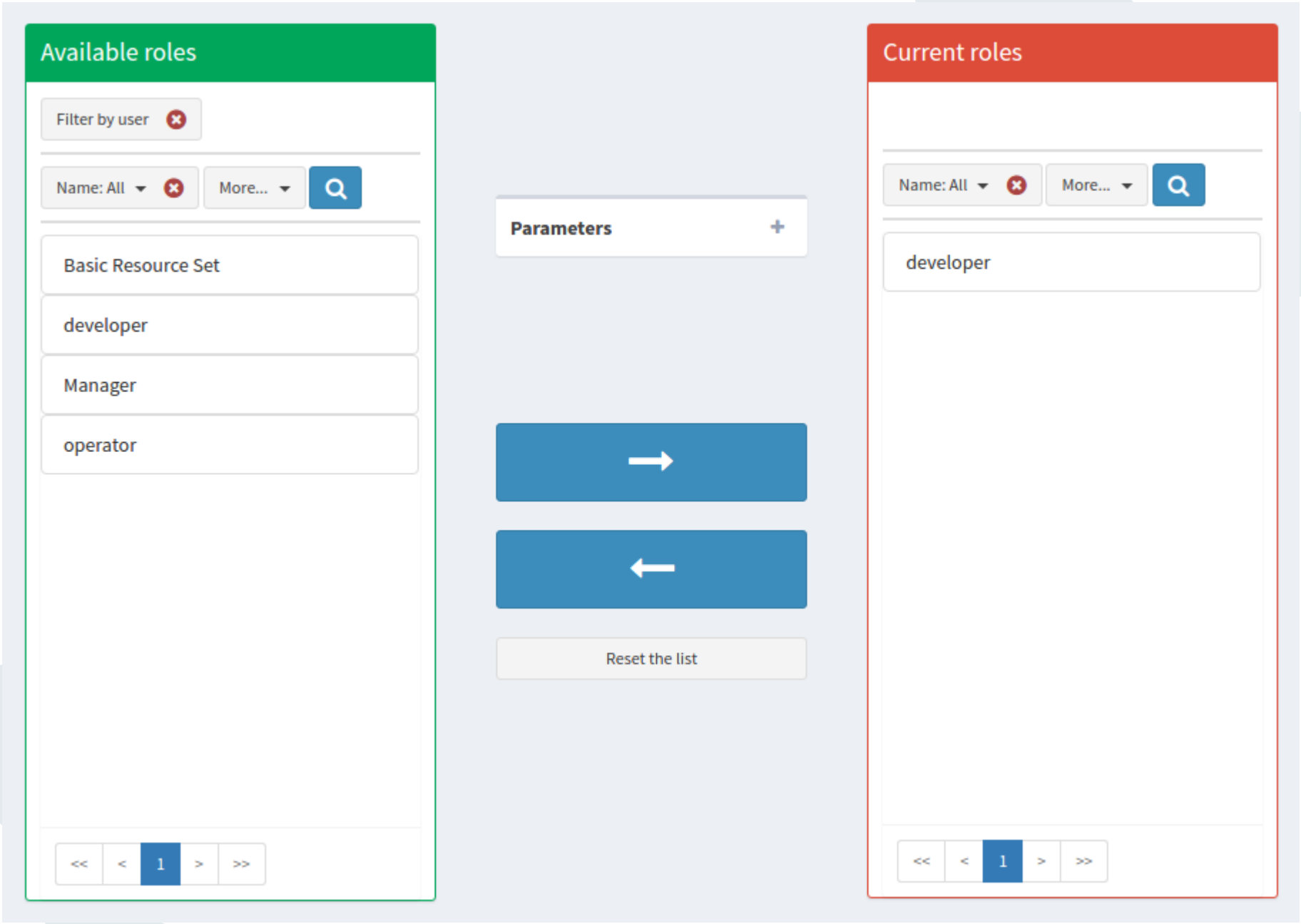



USERS
12 enabled
13 total
ORGANIZATIONAL UNITS
9 enabled
9 total
ROLES
5 enabled
6 total (+ 1 archived)
SERVICES
1 enabled
1 total
RESOURCES
2 up
5 total
TASKS
3 active
10 total

User details



Role request



Approve adding Sensitive Role 1 to katkav

Allocated

Requested by: katkav

Requested on: Apr 25, 2016 11:11:39 AM

Basic information

Requested by:	**katkav** (Ing. Katarína Valaliková)
Requested on:	**Monday, April 25, 2016 11:11:39 AM +02:00**
This work item created on:	**Monday, April 25, 2016 11:11:39 AM +02:00**
Allocated to:	**administrator**
Candidate actors:	

Changes waiting to be approved

Modify User Ing. Katarína Valaliková (katkav)

Add Assignment

Item	Value
Target	Sensitive Role 1

Show the approval request.

Approver comment

Back | Reject | Approve

Kind	Object Class	Intent	Synchronization	Tasks
ACCOUNT	inetOrgPerson		true	
ENTITLEMENT	groupOfNames	ldapGroup	true	
ENTITLEMENT	posixGroup	posixGroup	true	

1 to 3 of 3 << < 1 > >>

Live demo

http://demo.evolveum.com/

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

Clients and partners

Our clients

Open Data Node

CENTRUM VEDECKO-TECHNICKÝCH INFORMÁCIÍ SR

PosAm

TÜBİTAK

Union
Poisťovňa

UNIVERZITA · SELYE JÁNOS EGYETEM

ami

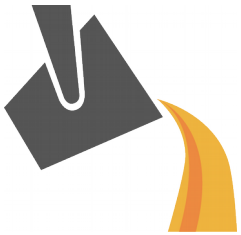
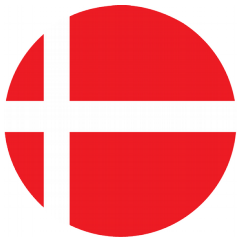
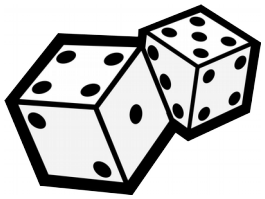
SKYIDENTITY

Česká televize

WWK
Eine starke Gemeinschaft

UNIVERSITAS COMENIANA BRATISLAVENSIS
MCMXIX

Our clients

Partners

Salfordsoftware
Identity as a service

BİZNET
BİLİŞİM

CIIT

ARTIN

ami

DAASI
International

komix

INTELILOGIX
INTELLIGENT SOLUTIONS

nLight

Servodata

GEM
SYSTEM

GAMO
INFORMAČNÉ TECHNOLÓGIE

INTERWAY
Your IT Way

innoBT

VERDE

osi.si
Open Systems Integration

Cogito Group

SOLID.TECHNOLOGY
NORTHWEST LLC

SYNTEGRITY
INTELLIGENT SECURITY

IDENTITY
WORKS LLC

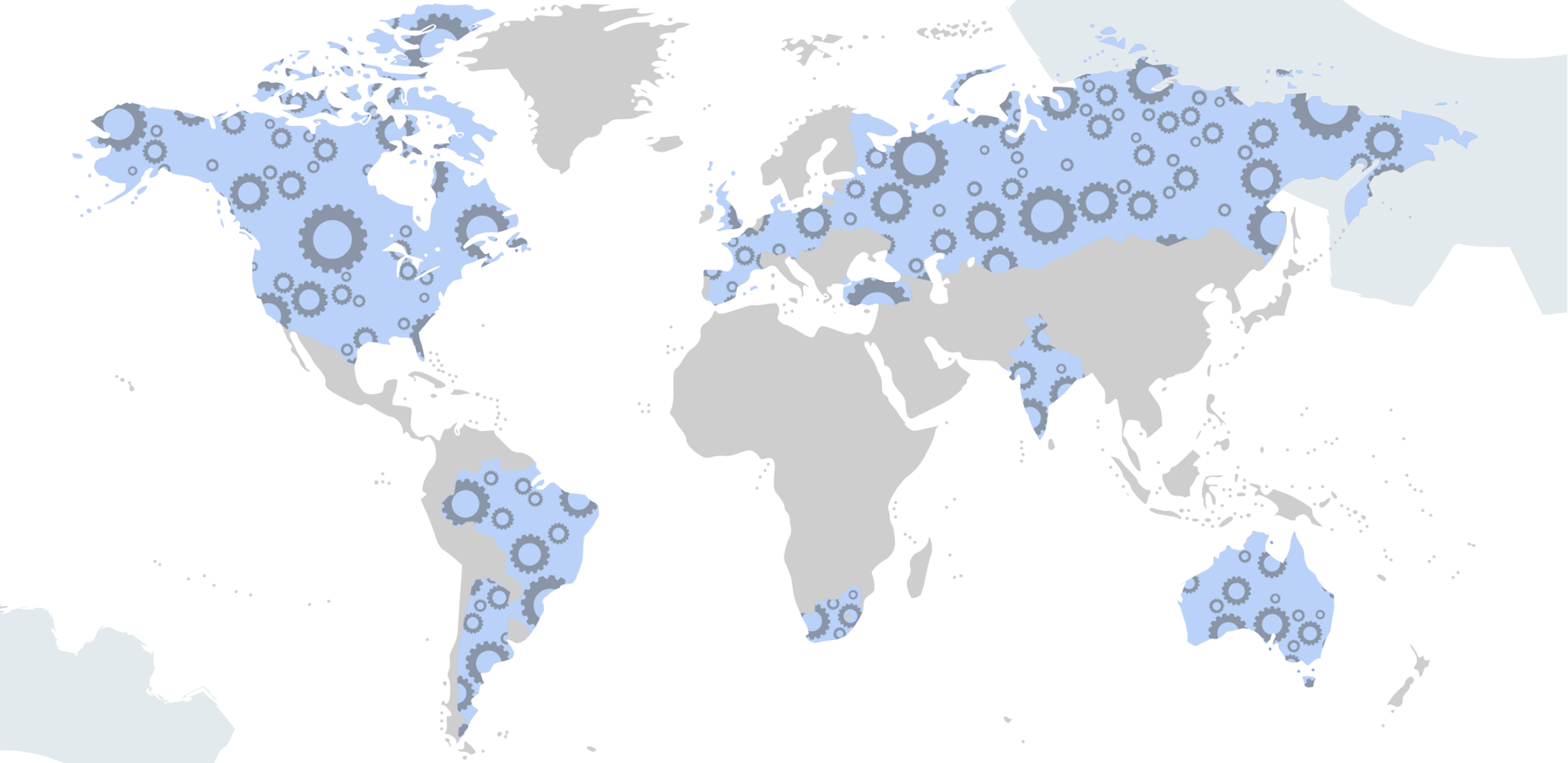
identicum

symas

IBA
GROUP

PSYND
IT SECURITY SERVICES

Countries where midPoint is used



Conclusion

Conclusion

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

If you have any questions,
please feel free to ask

Thank you for your attention