

Evolveum



MidPoint: Open Source Identity Governance

Radovan Semančík, April 2025
Software Architect

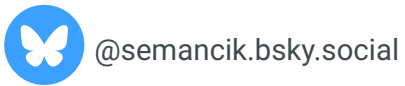
Agenda

- What is Identity Governance and Administration?
- What midPoint does?
- What is inside midPoint?
- What will future bring?

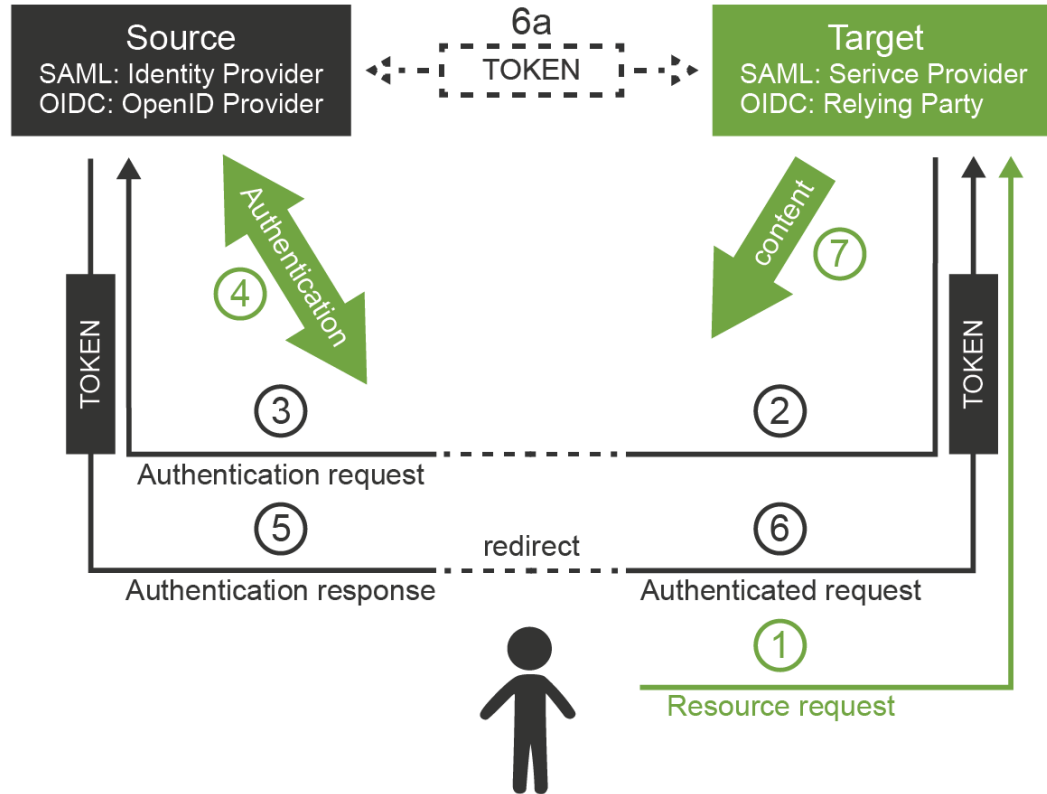


Radovan Semančík

- Software architect at Evolveum
- Open source (since 20th century)
- Identity (since 2000s)
- Retired Apache committer and PMC



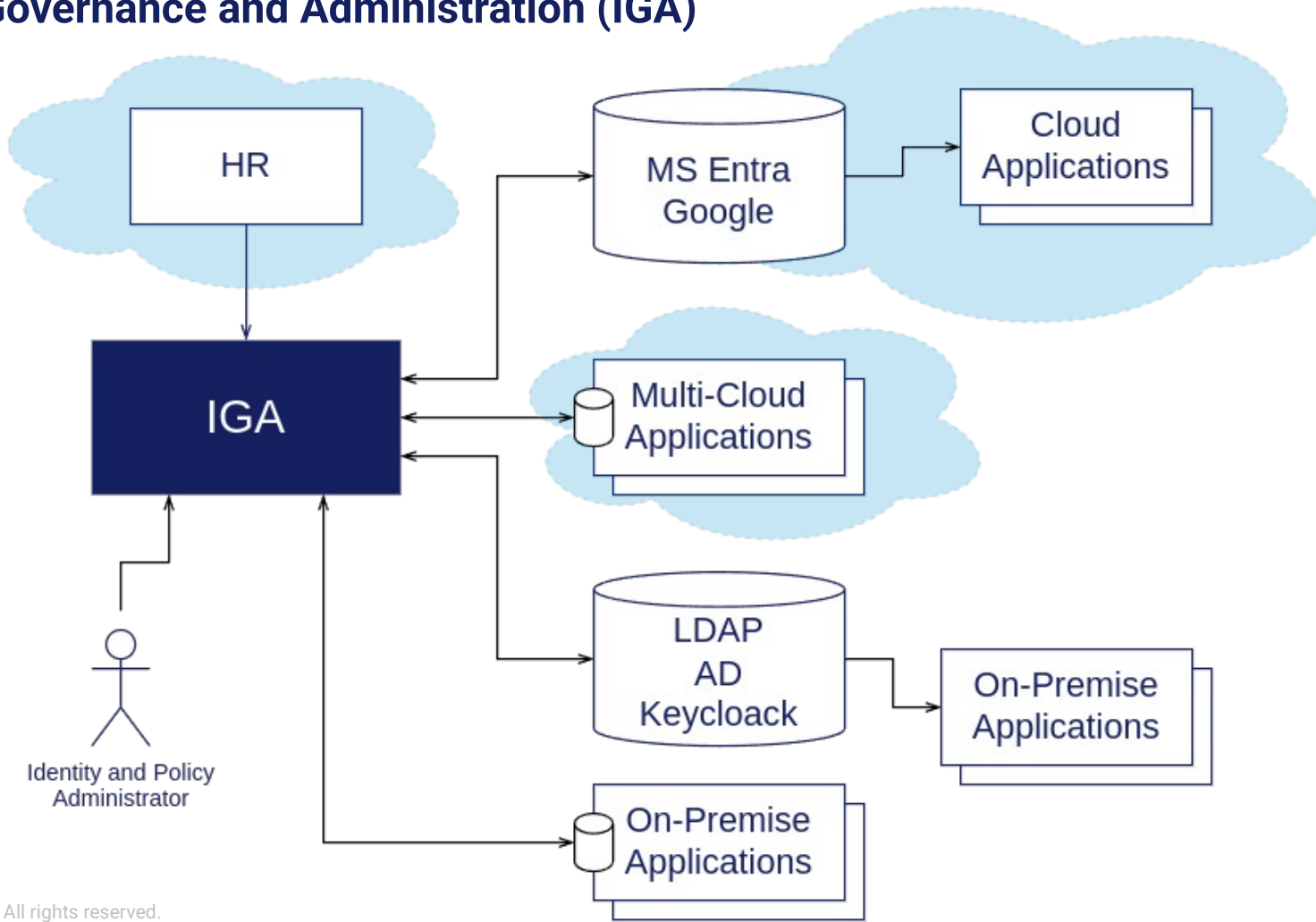
“Identity”: Access Management, Single Sign-On, Authentication, Federation, ...



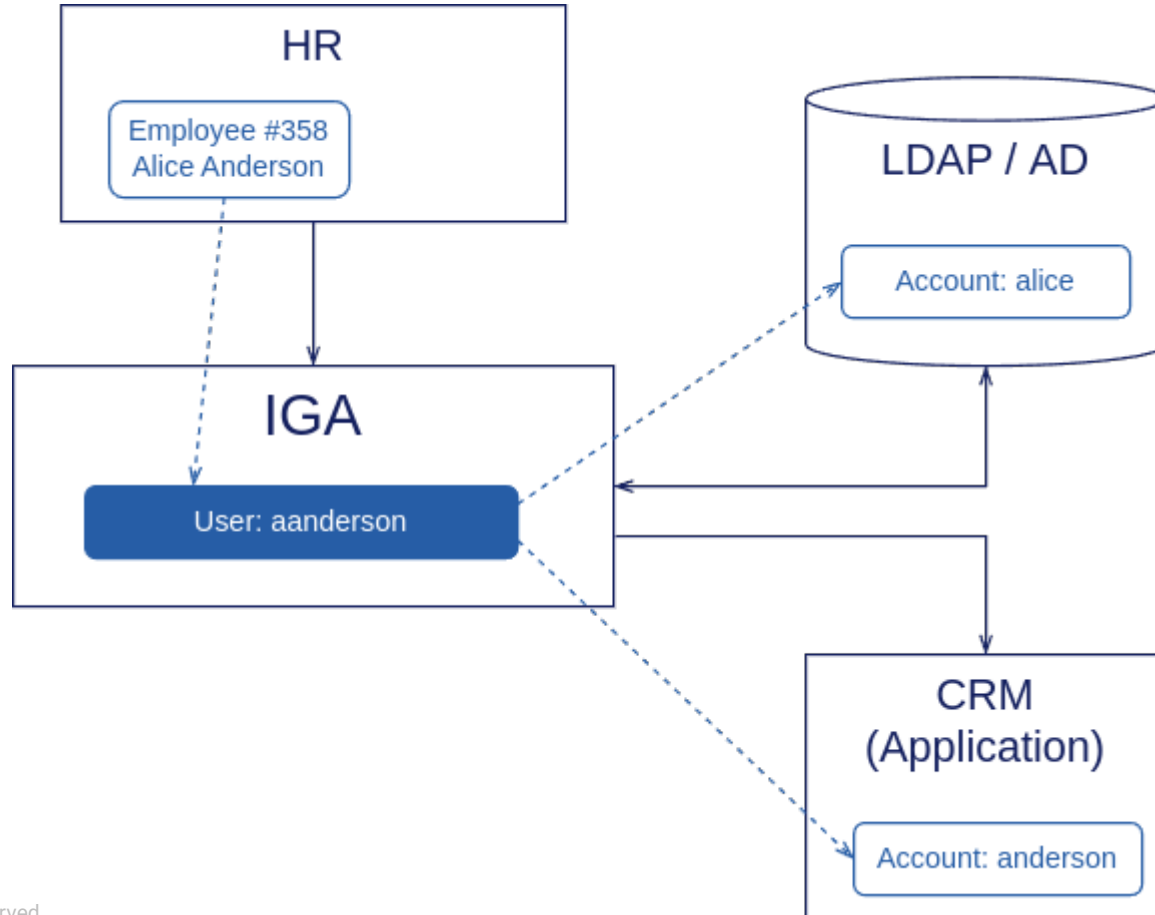
- OpenID Connect, OAuth2
- SAML
- WebAuthn, FIDO2
- ...

This is not Identity
Governance and Administration
(IGA)

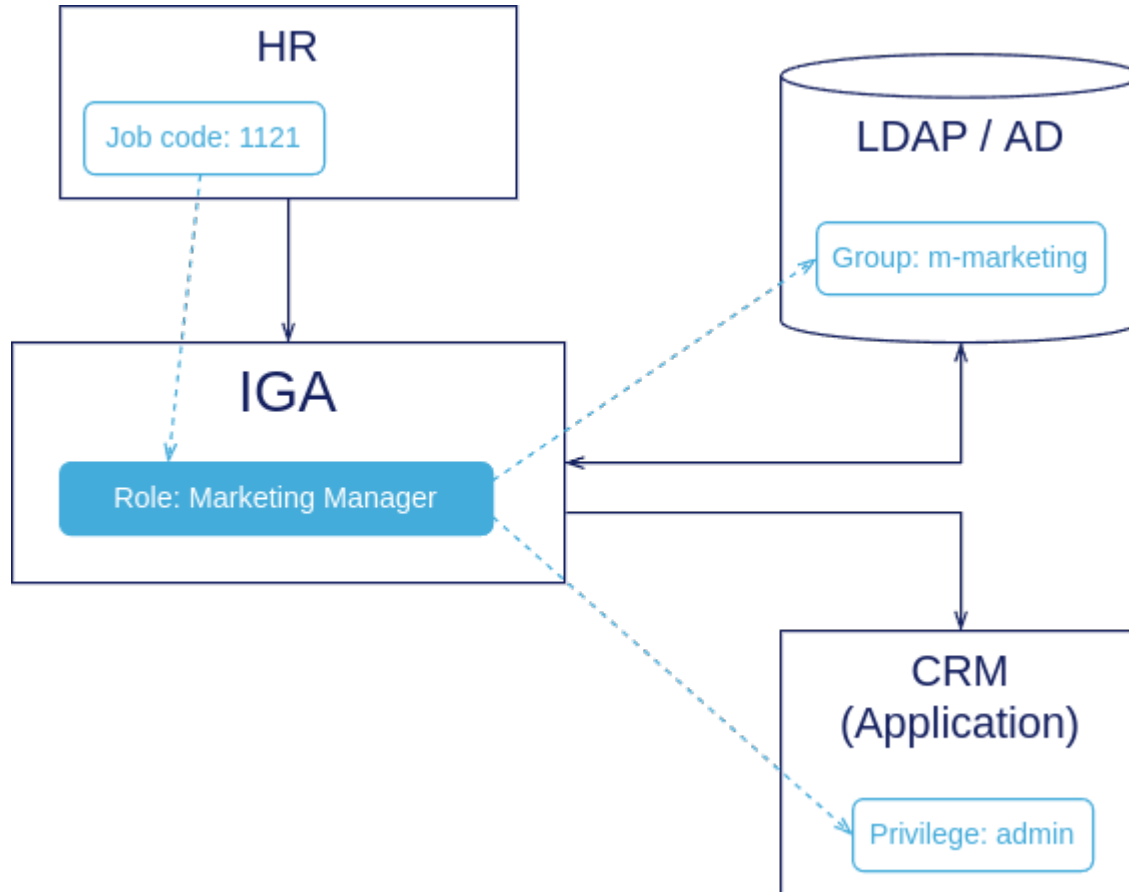
Identity Governance and Administration (IGA)



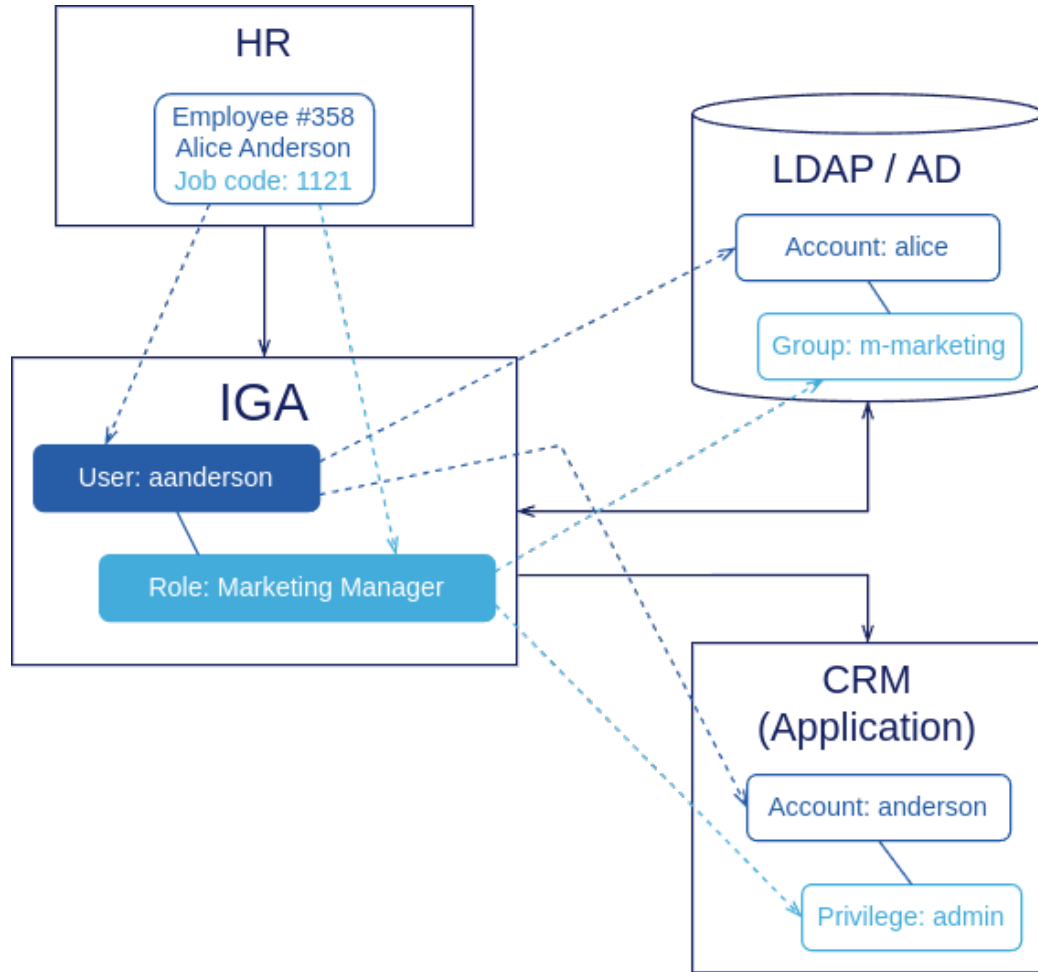
IGA: Identity Lifecycle Management



IGA: Entitlement Management



IGA: Identities and Entitlements



Basic Security Features of IGA

- Orphaned account detection
 - Entitlement management
 - Role-based access control (RBAC)
 - Segregation of duties (SoD)
 - Outlier detection
 - Audit trail
 - Visibility, visibility, visibility!
- Identity lifecycle management
 - Owners: roles, groups, privileges
 - Policy management
 - Assignment metadata
 - Access request and approval
 - Access review (certification)
 - Information classification



Governance?

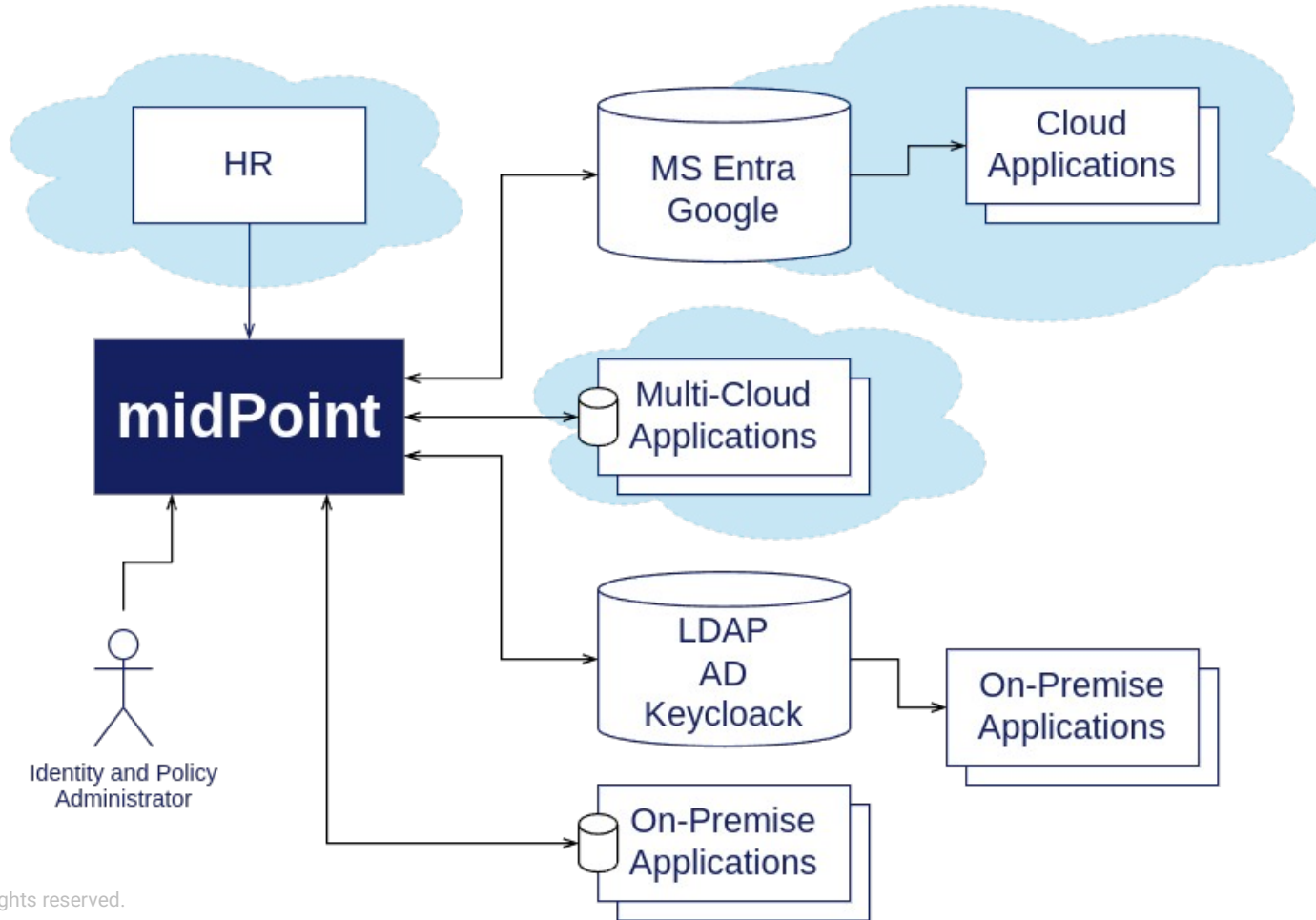
- Identity management administration → governance
- Identity management/administration: low-level policies, access control
- Identity governance: high-level policies
 - Ownership, responsibility
 - Inventory
 - Risk management
 - Compliance (ISO27001, NIS2, DORA, NIST CSF, ...)



If you do not have **identity governance**,
you have no cybersecurity.

Cybersecurity is all about *users* - their actions, permissions, the value they create and the risk they are posing. If you do not control the *users*, you control nothing. All your cybersecurity is just an illusion.

MidPoint IGA Platform



MidPoint IGA Platform

midPoint

All users

Users > All users



administrator

SELF SERVICE

Home

Profile

Credentials

Request access

ADMINISTRATION

Dashboards

Users

All users

Persons

New user

Org. structure

Roles

Services

Object collection

Undefined

Full name

Name

More...

Basic

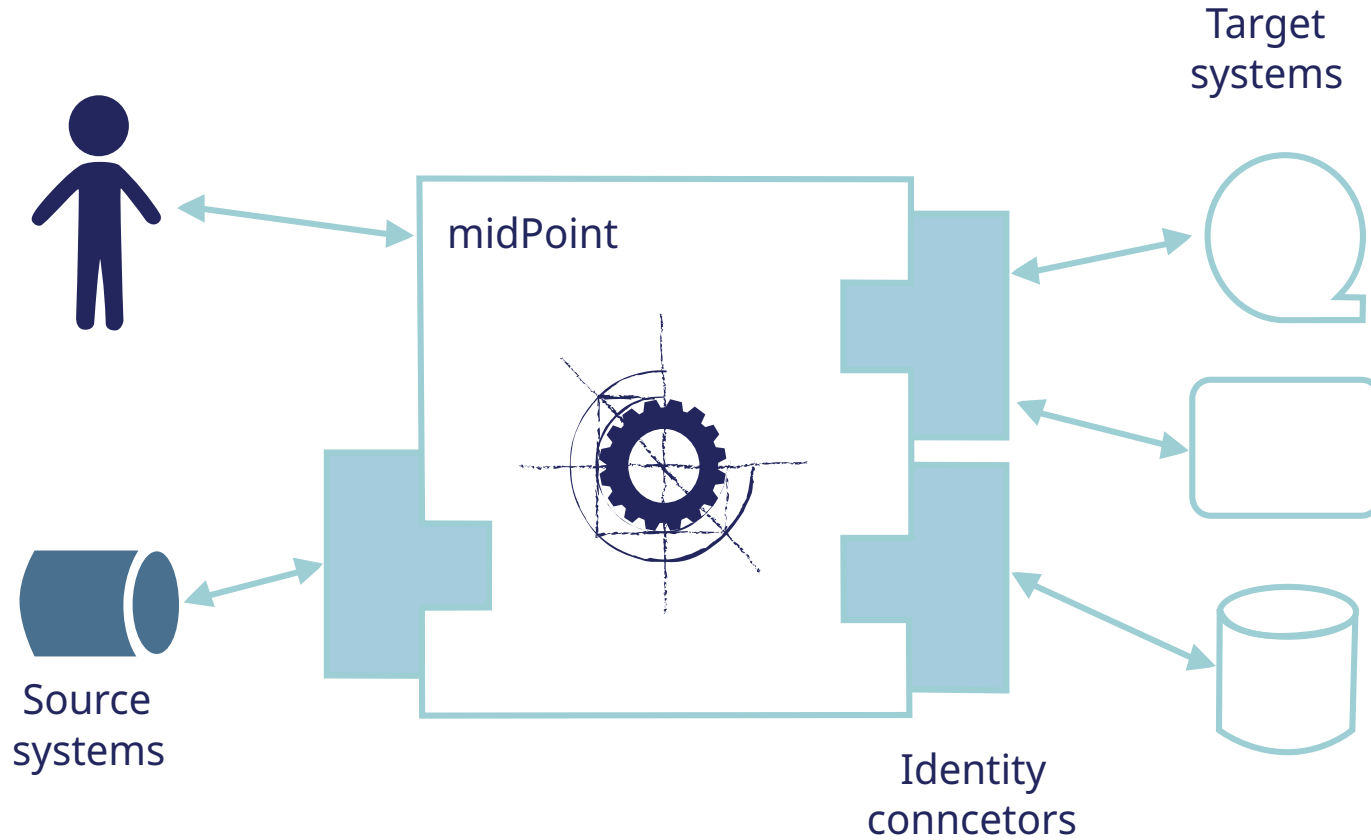
| <input type="checkbox"/> | Name | Personal Number | Full name | Email | Accounts | |
|--------------------------|---------------|-----------------|------------------------|-----------------------------|----------|--|
| <input type="checkbox"/> | aanderso | 001 | Alice Anderson | alice.anderson@example.com | 2 | |
| <input type="checkbox"/> | administrator | | midPoint Administrator | | | |
| <input type="checkbox"/> | brown | 002 | Bob Brown | bob.brown@example.com | 2 | |
| <input type="checkbox"/> | carol | 003 | Carol Cooper | carol.cooper@example.com | 2 | |
| <input type="checkbox"/> | davies | 004 | David Davies | david.davies@example.com | 2 | |
| <input type="checkbox"/> | eevans | 005 | Erin Evans | erin.evans@example.com | 2 | |
| <input type="checkbox"/> | ffox | 006 | Frank Fox | frank.fox@example.com | 2 | |
| <input type="checkbox"/> | ggreen | 007 | George Green | george.green@example.com | 2 | |
| <input type="checkbox"/> | hharris | 008 | Harry Harris | harry.harris@example.com | 2 | |
| <input type="checkbox"/> | iirvine | 009 | Isabella Irvine | isabella.irvine@example.com | 2 | |
| <input type="checkbox"/> | jjones | 010 | Jack Jones | jack.jones@example.com | 2 | |

MidPoint Project

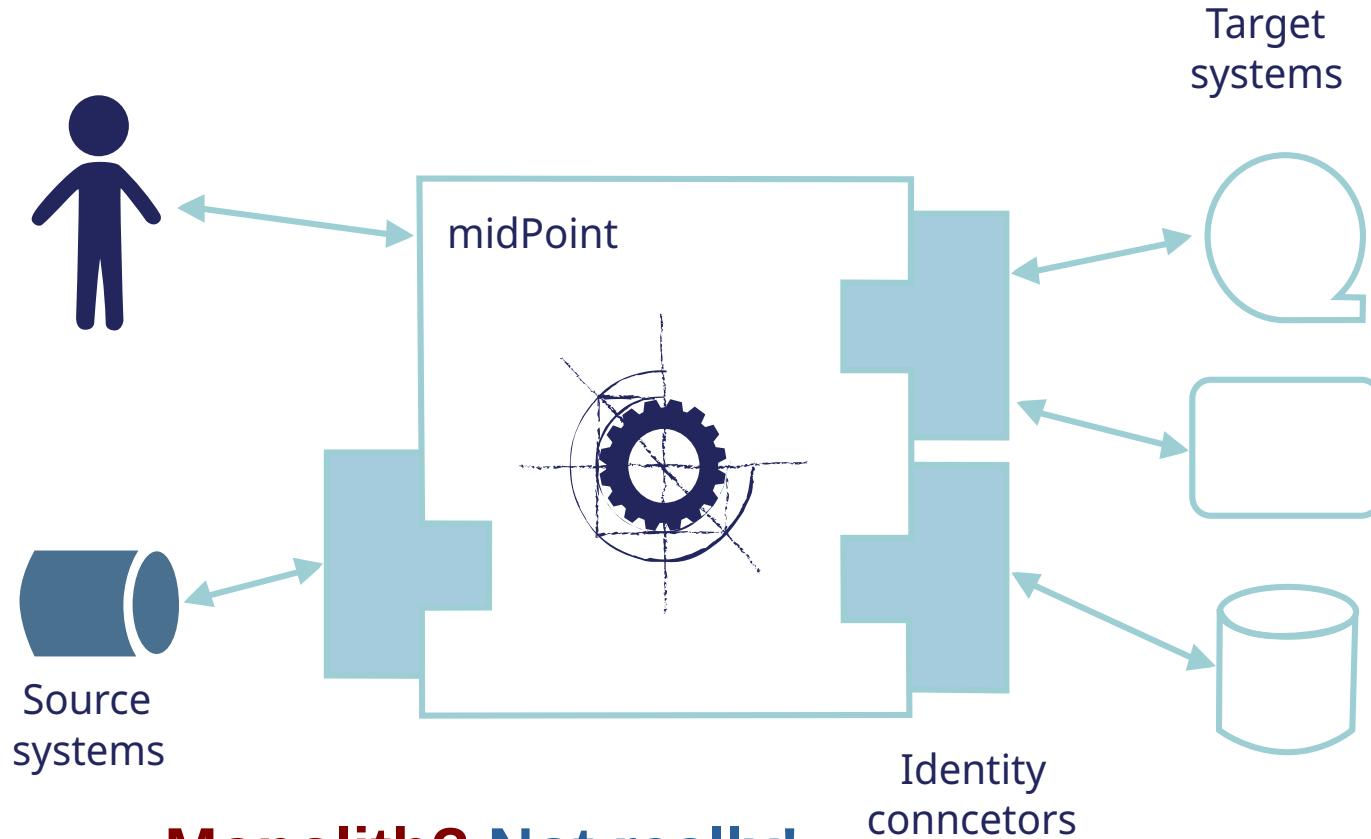
- Identity Governance and Administration (IGA) platform
- Since 2011 (14 years)
- Open source (Apache License + EUPL)
- Java (1M+ SLOC)
- Public documentation
- Book
- Self-funded (no investor), profitable

midPoint

Look Inside MidPoint



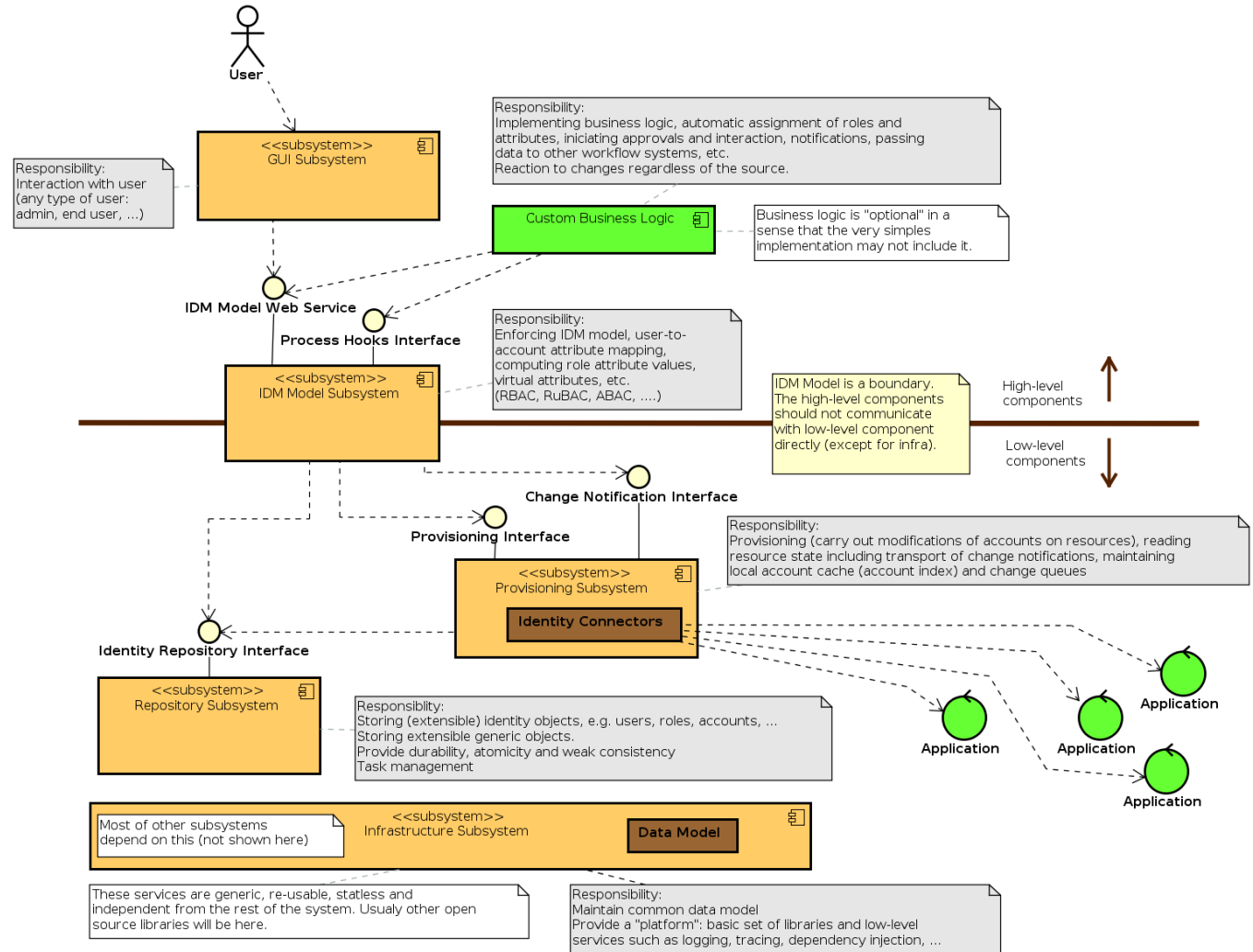
Look Inside MidPoint



Monolith? Not really!

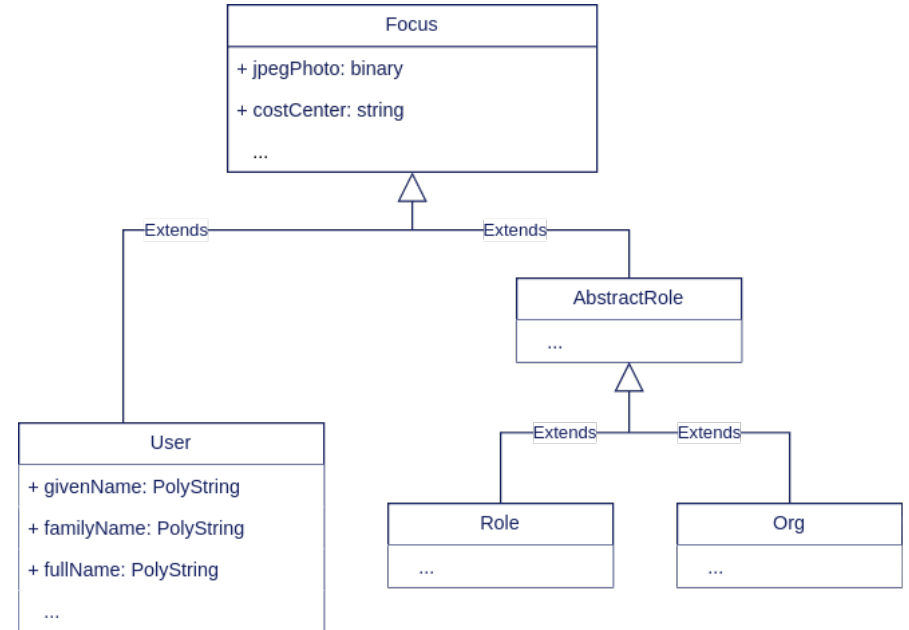
MidPoint Architecture

- Subsystems
- Components
- Interfaces
- Modules (connectors)

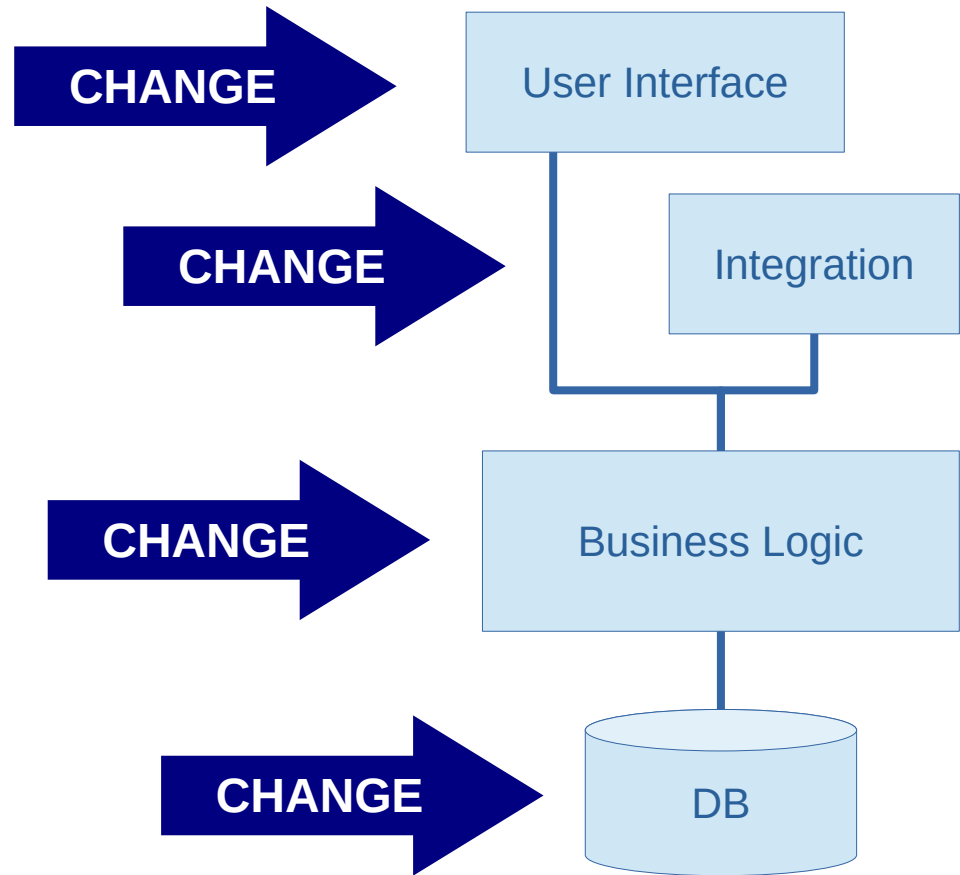


Data Model

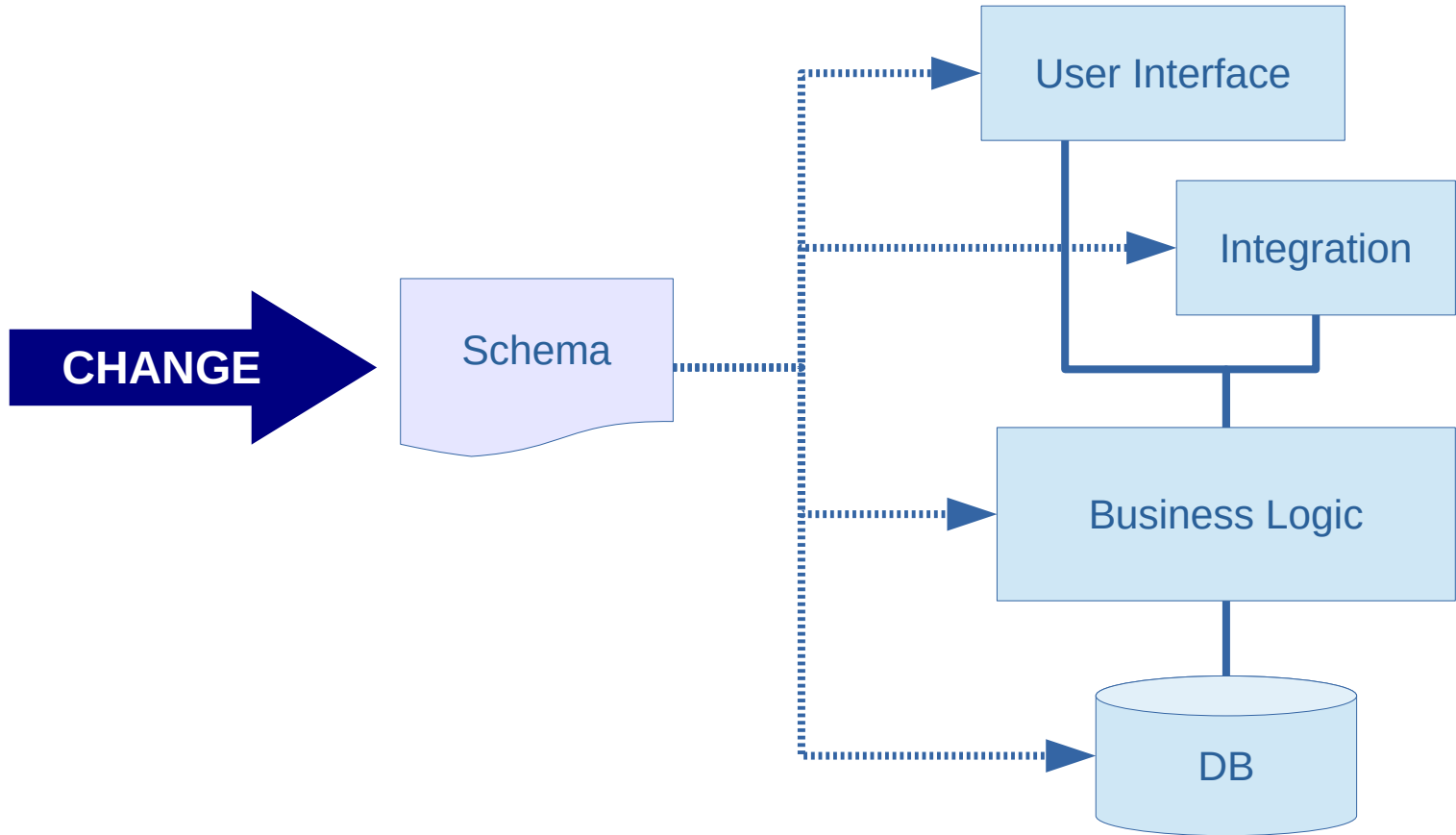
- Extremely important
- As important as architecture
- Cross-cutting concern
- Performance, scalability, evolvability, ...
- Changes often - especially at the beginning
- Evolution - compatibility - upgrades
- Experimental features



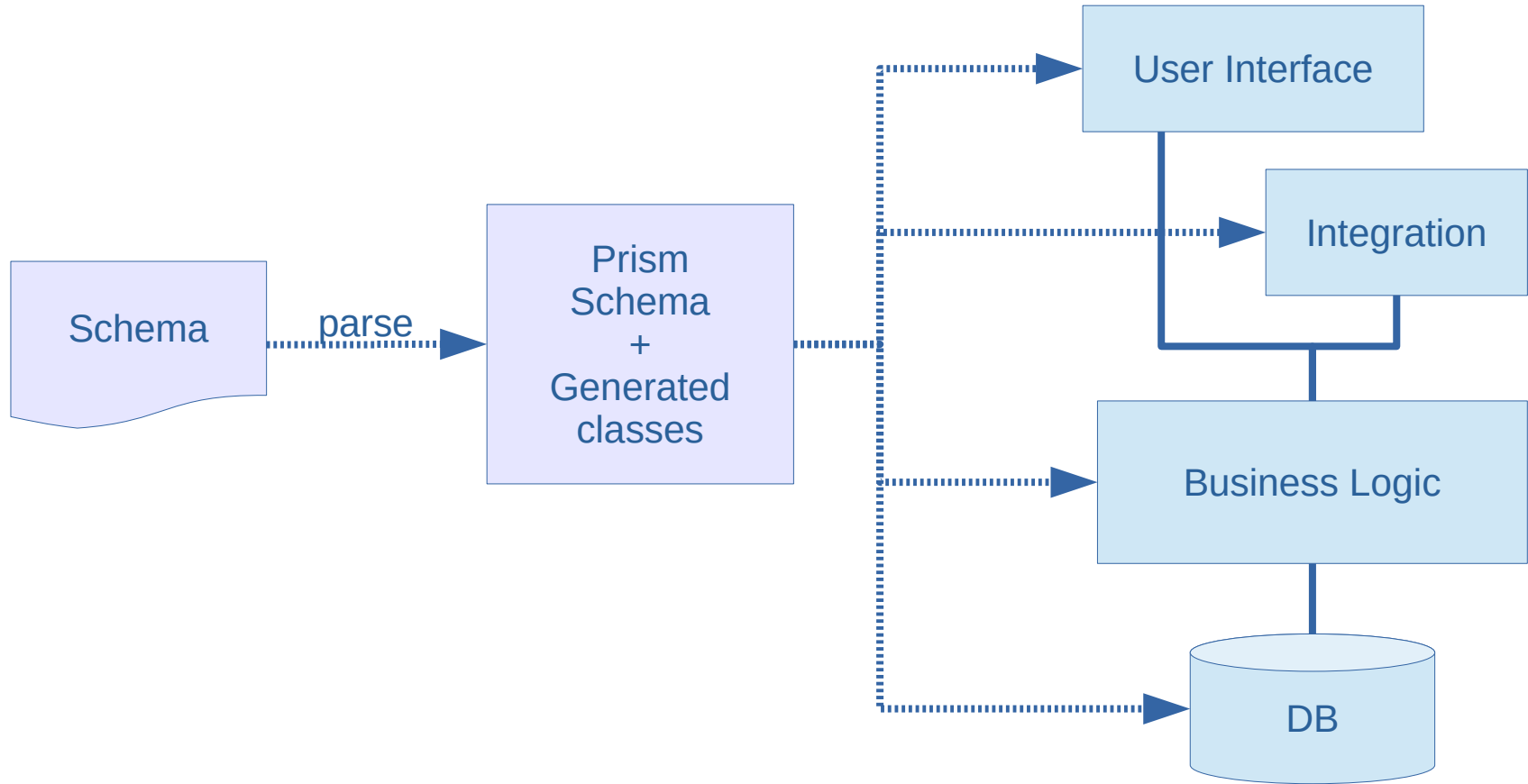
Data Model: Change



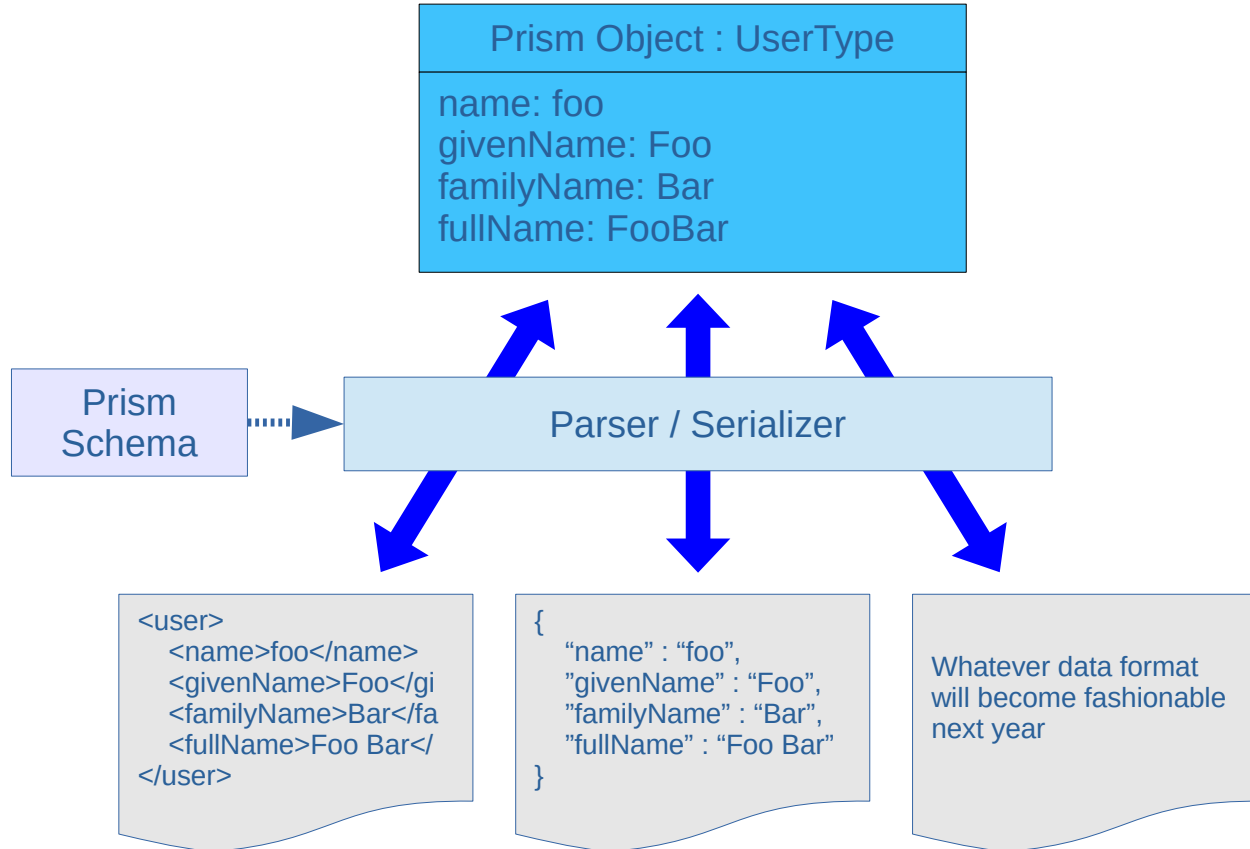
Data Model: Schema Change



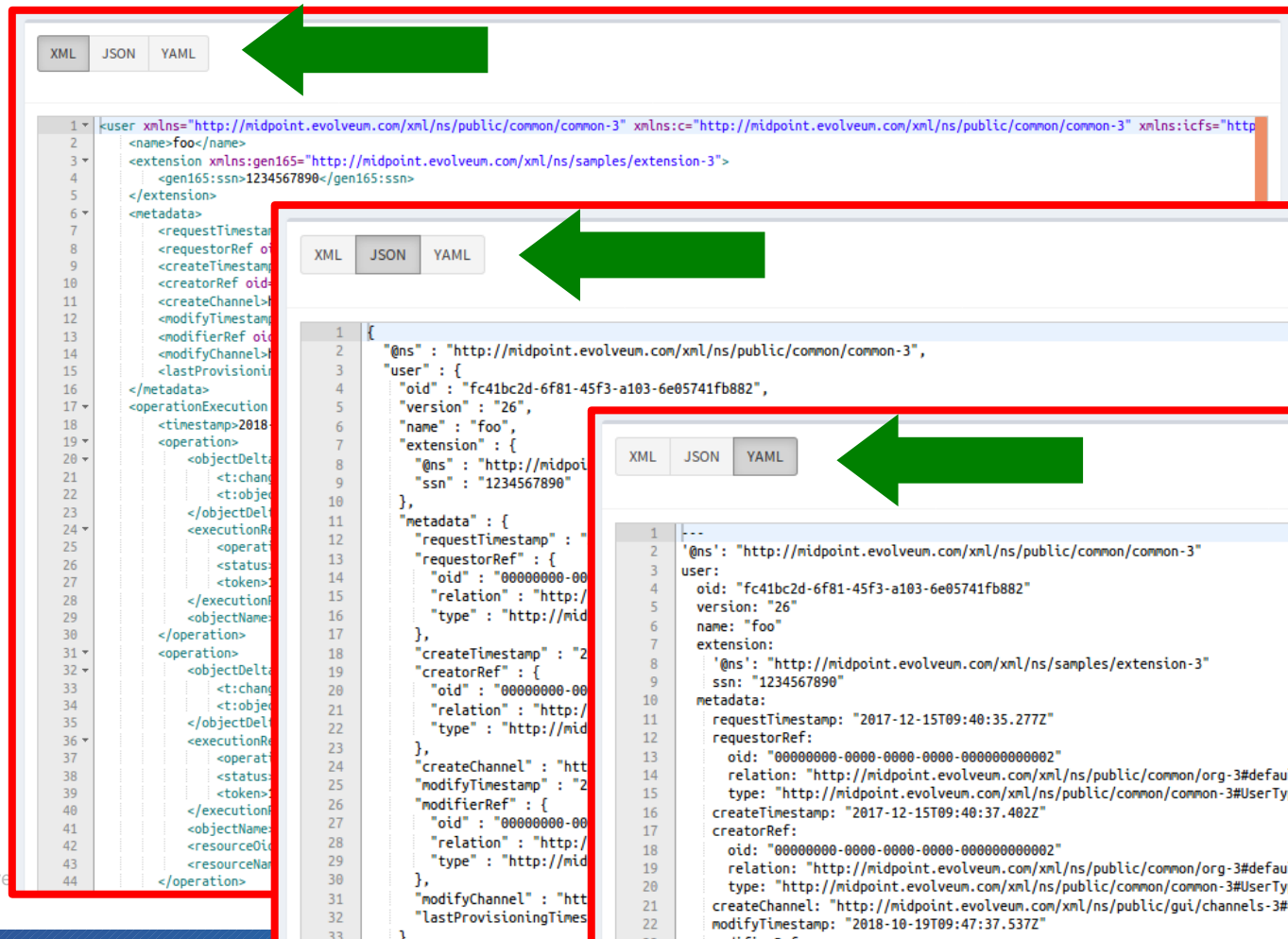
Data Model: Schema Change



XML, JSON, YAML and Friends



XML, JSON, YAML and Friends



The image displays three panels illustrating the conversion of XML data to JSON and then to YAML. Each panel shows a source code editor on the left and the rendered output on the right.

XML Panel (Left): The source code editor contains XML. The output pane shows the rendered XML structure, including namespace declarations and nested elements like `<user>`, `<extension>`, `<metadata>`, `<requestTimestamp>`, `<requestorRef>`, `<createTimestamp>`, `<creatorRef>`, `<createChannel>`, `<modifyTimestamp>`, `<modifierRef>`, `<modifyChannel>`, `<lastProvisioningTime>`, `</metadata>`, `<operationExecution>`, `<timestamp>`, `<operation>`, `<objectDelta>`, `<t:change>`, `<t:objectName>`, `</objectDelta>`, `<executionReference>`, `<operation>`, `<status>`, `<token>`, `</executionReference>`, `<objectName>`, `</operation>`, `<operation>`, `<objectDelta>`, `<t:change>`, `<t:objectName>`, `</objectDelta>`, `<executionReference>`, `<operation>`, `<status>`, `<token>`, `</executionReference>`, `<objectName>`, `<resourceId>`, `<resourceName>`, `</operation>`.

JSON Panel (Middle): The source code editor contains JSON. The output pane shows the rendered JSON structure, including namespace declarations and nested objects like `user`, `extension`, `metadata`, `requestTimestamp`, `requestorRef`, `createTimestamp`, `creatorRef`, `createChannel`, `modifyTimestamp`, `modifierRef`, `modifyChannel`, `lastProvisioningTime`, `operationExecution`, `timestamp`, `operation`, `objectDelta`, `t:change`, `t:objectName`, `executionReference`, `operation`, `status`, `token`, `objectName`, `resourceId`, `resourceName`.

YAML Panel (Right): The source code editor contains YAML. The output pane shows the rendered YAML structure, including namespace declarations and nested objects like `user`, `extension`, `metadata`, `requestTimestamp`, `requestorRef`, `createTimestamp`, `creatorRef`, `createChannel`, `modifyTimestamp`, `modifierRef`, `modifyChannel`, `lastProvisioningTime`, `operationExecution`, `timestamp`, `operation`, `objectDelta`, `t:change`, `t:objectName`, `executionReference`, `operation`, `status`, `token`, `objectName`, `resourceId`, `resourceName`.

Prism: Much more

- Static schema (compile-time)
- Dynamic schema (run-time)
- “Superdynamic” schema
 - Raw data, we do not have complete schema at parse-time
- Deltas (schema-aware)
- Search filters (schema-aware, of course)
- Lifecycle (versioning, deprecated, experimental)



Dependencies

How it started (~2012)

- Spring
- Java Server Faces
- XML (DOM)
- JAX-B
- JAX-WS
- ESB/BPEL, Activiti BPM
- Jasper Reports
- Hibernate
- ...

how is it going (2025)

- Spring + Spring Boot
- Apache Wicket
- XML (DOM) + JSON + YAML
- ~~JAX-B~~
- ~~JAX-WS~~
- ~~ESB/BPEL, Activiti BPM~~
- ~~Jasper Reports~~
- ~~Hibernate~~
- ...

CRA (2027)

- Spring + Spring Boot
- Apache Wicket
- XML (DOM) + JSON + YAML
- ???
[Reduce]
[Reduce]
[Reduce]

Dependencies: Lessons Learned

- Faster start of the project
- Do not reinvent the wheel
 - ... unless the wheel is in fact a square
- Do not depend on dependencies too much
- Understand how they work – and why they fail
- Reduce dependencies as project matures
- Cyber Resilience Act: 2027



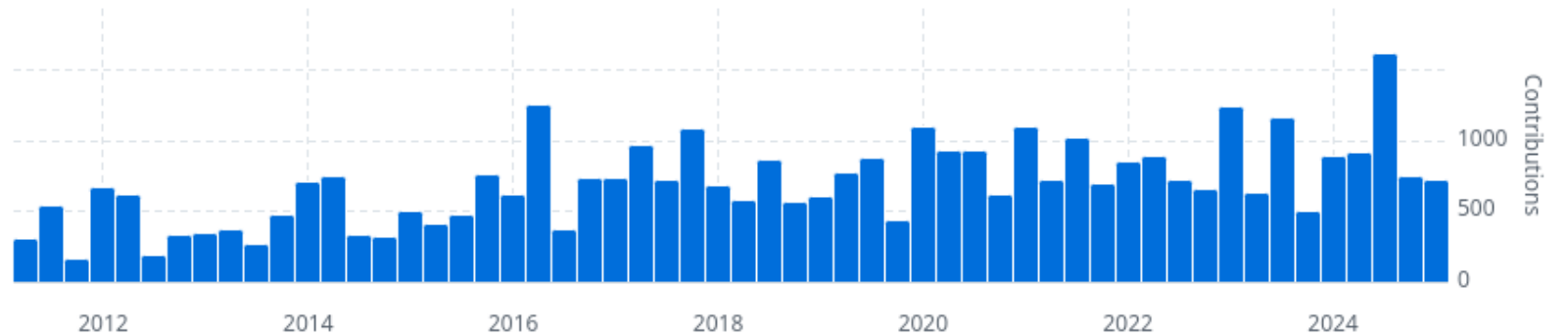
Development

<https://github.com/Evolveum/midpoint>

- Evolutionary approach (iterative & incremental)
- High development activity
- 7 professional full-time developers + engineers, etc.
- Skills: Java, UX (Figma), HTML/CSS, JavaScript, AI, CI/CD, Testing, DevOps, ...
- We are hiring!

Commits over time

Weekly from May 8, 2011 to Mar 16, 2025



Future

- Development never stops
- World is changing
 - Cybersecurity crisis: Cyber Resilience Act (CRA)
 - Trump crisis: European digital sovereignty
- Software is never going to be the same again
- Open source for the win?
- Funding?



Thank you for your attention

MidPoint Community Meetup

Bratislava, 12-14 May 2025



/semancik



@semancik.bsky.social



/semancik

Evolveum

© 2025 Evolveum s.r.o. All rights reserved.