



## **Role of IGA in Access Management with Multilateral Identities**

**Slávek Licehammer**

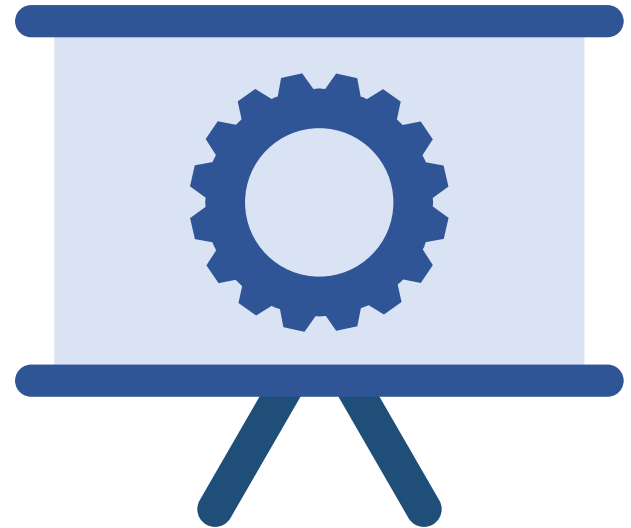
Evolveum's Identity Governance Strategist  
and Global Leader for Academia

# Introduction

- Multilateral identities
  - Identities from multiple different sources
  - Institutional, state, social, academic, bank, ...
- Access management
  - Use identities for providing access to service
- IGA
  - Extension of IdM towards non-technical people
  - In this talk represented by midPoint



- Mature IGA and IdM system
- Fully open-source
  - Including documentation, modules, guidelines, etc.
- Maintained by Evolveum
  - Few external contributors
- Feature rich
  - Up to par with commercial products
- Fully customizable, uses standards
- <https://evolveum.com/midpoint/>



# Access Management Integration

- IGA → Access management
  - Profile information
  - Authorization data
- Access management → IGA
  - Identities and attributes
  - Access timestamps
- Typical interfaces
  - IGA provision/synchronize with access management
  - Access management calls IGA's API



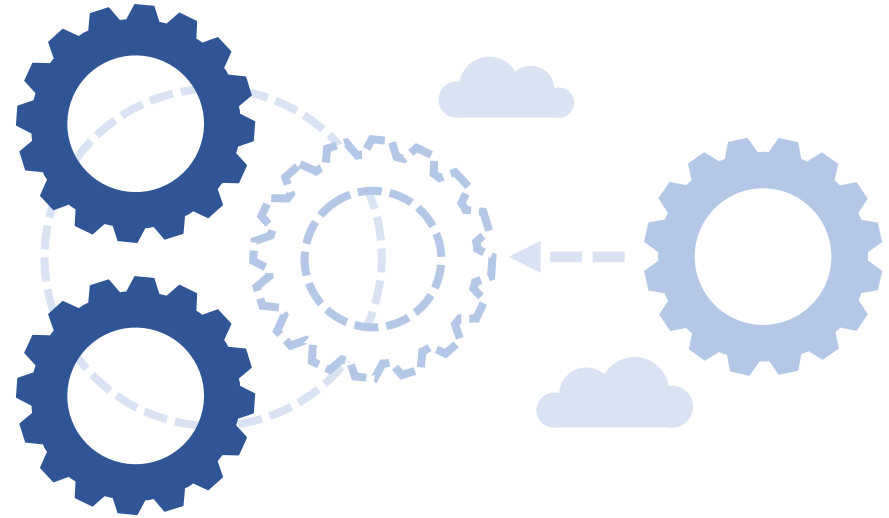
## IGA Benefits

- Visibility
  - Who has access to what and why
  - Reporting, auditing
- Policy driven RBAC
  - Use attributes from various identities
  - Remove unused accounts
- Automation
  - (De-)provisioning
  - Approvals



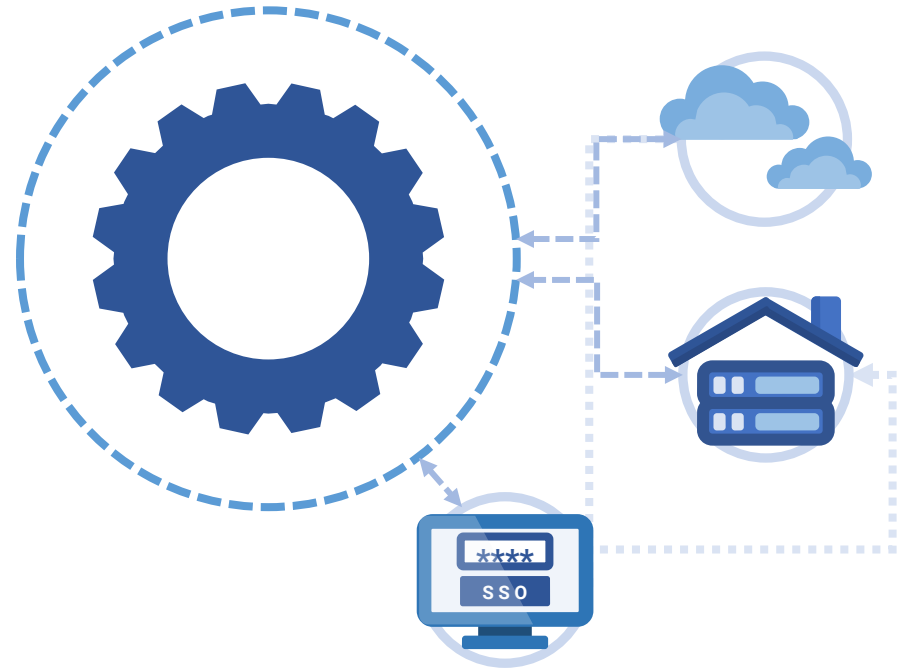
## Just in Time Provisioning with Access Management

- Create account during first sign-in
- Requires support by target system
- Authorization done on access management level
- Difficult deprovisioning
- Limited visibility and control



## Just in Time Provisioning with midPoint

- MidPoint manages entitled users
- Access management (AM) get authorization data
- AM request JIT account activation though midPoint
  - Or use native JIT capability of target system
- MidPoint has integration with target
  - Knows about active accounts
- MidPoint can deprovision later



## MidPoint with Multilateral Identities

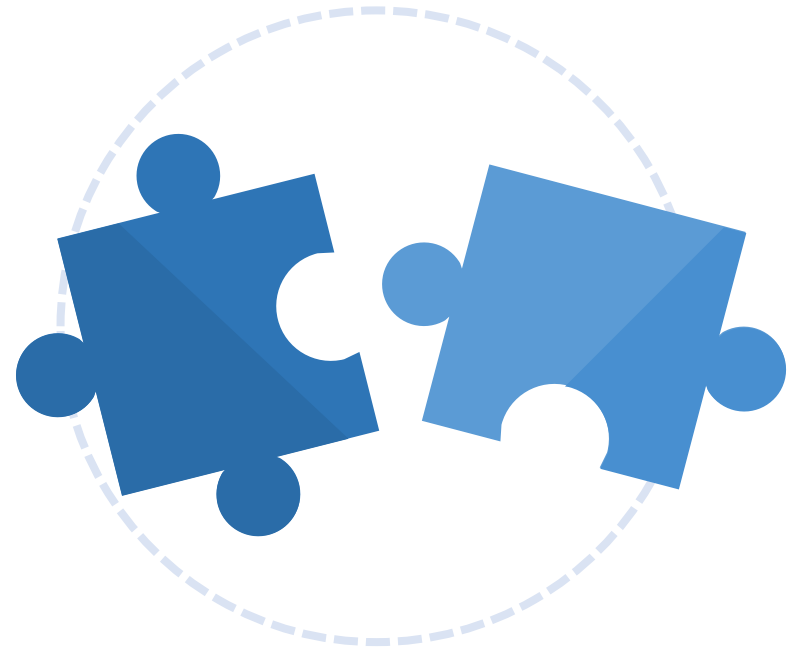
- Multi-identities
  - Smart correlation
  - Correlation at access management level possible
- Combining internal and external identities
- Unified profile
  - Based on rules and user preferences
  - Comply to organizational policies
- Fully automated processing





## Missing Pieces

- User experience
- Well-defined interface between IGA and AM
- Whole life-cycle of an identity
- Assurance and trust models might be complex
  - MidPrivacy project
  - <https://docs.evolveum.com/midpoint/projects/midprivacy/>



## Conclusion

- It's possible to combine IGA with access management
- There are lot of existing identities that can be used
- IGA adds order to distributed world of multilateral identities
- Full implementation is complex
- MidPoint is half way through
- Contributions and collaboration is welcome



# Thank you for your time

Do you have any **questions**? Feel free to contact me at [slavek@evolveum.com](mailto:slavek@evolveum.com)

**Follow us** on social media or **join us** at GitHub or Gitter!



**Evolveum**

© 2024 Evolveum s.r.o. All rights reserved.