



**Governing Non-Human Identities with Proven IGA Principles**

Slávek Licehammer, May 2025  
Head of Engineering

# Agenda

- Introduction to non-human identities (NHI)
- Management of NHI
- Governance of NHI
- Conclusion and recommendation



## From Human to Non-Human Identities (NHI)?

- Human identities are prime
- NHI are naturally occurring
- Modern IT is mostly automatized
- Blurring the differences
  - Devices, services, agents acting as a user
- Zero trust principles
- Embrace non-human identities



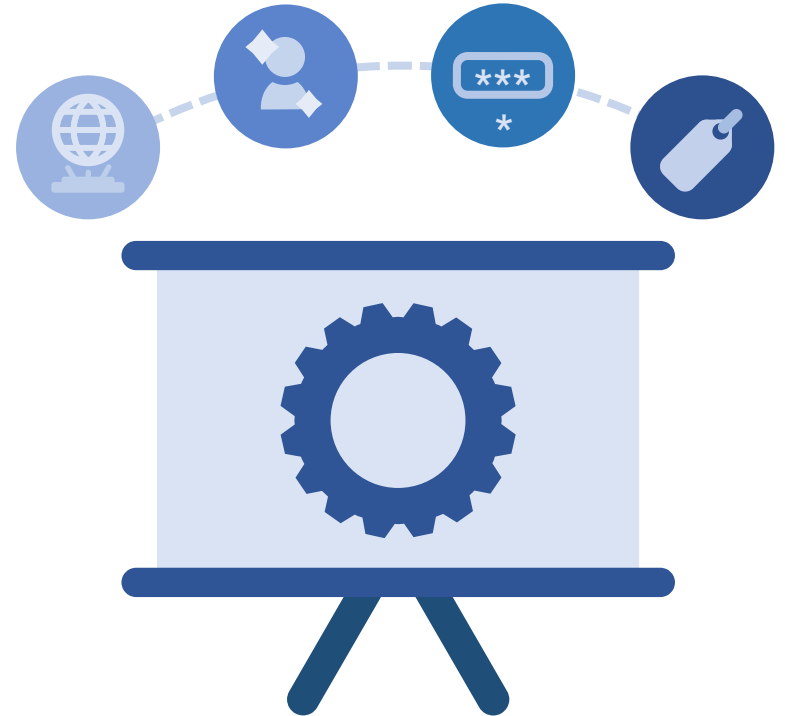
# Why Non-Human Identities?

- The number is rising
  - Estimates are 20-50x more than human identities
- Often overlooked
  - Both life-cycle and usage
- Huge potential attack surface
  - Privileged by design
- Harder to manage
  - Scale
  - Shared ownership



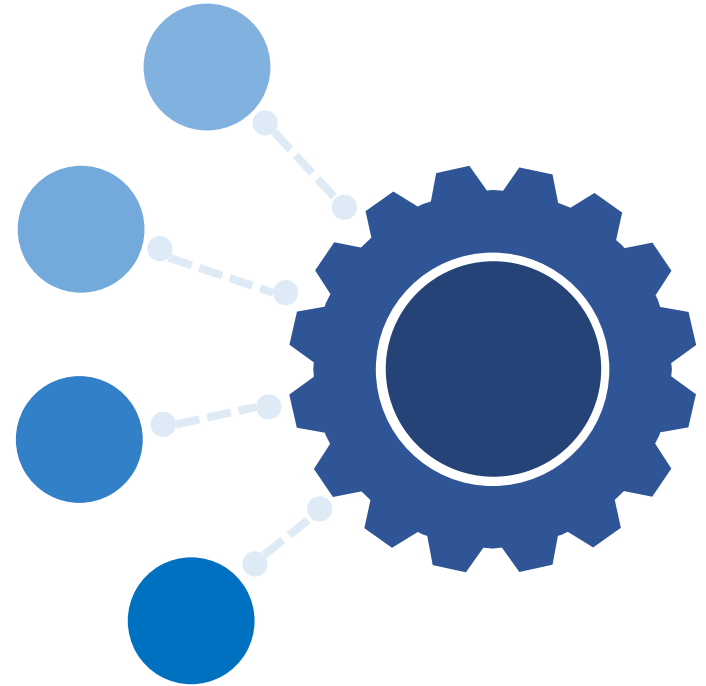
## Types of Non-Human Identities

- Service accounts, system accounts
- Devices
- Internet of things
- Applications, micro-services
- Agents, bots
- Integration code, CI/CD
- Workload
- ...



## Typical Approach to Non-Human Identities

- Low-level approach to NHI management
- Security
- Credential management
- API protection
- Monitoring, risk assessment
- There are many specialized solutions for it



## A Different View of NHI

- Evolveum focuses on IGA
- MidPoint
- Open source IGA platform made in EU
- Thinking about NHI from the IGA point of view

The screenshot displays the MidPoint web interface for user management. The left sidebar contains a navigation menu with options like SELF SERVICE, ADMINISTRATION, Dashboards, Users (selected), All users, Persons, Agents, Devices, Service acc., New user, Org. structure, Roles, Services, Policies, Resources, Cases, Certification, and Server tasks. The main area shows a table of users with columns for Name, Personal Number, Full name, Email, and Accounts. The table lists several users, including 'administrator', 'borgia', 'ci/cd-agent', 'db-admin', 'donatello', 'francis', 'hallway-scanner', and 'ldap-administrator'.

	Name	Personal Number	Full name	Email	Accounts
<input type="checkbox"/>	administrator		midPoint Administrator		
<input type="checkbox"/>	borgia		Cesare Borgia	cborgia@leonardo-workshop.org	
<input type="checkbox"/>	ci/cd-agent	NHI-4	CI/CD integration agent	it@leonardo-workshop.org	4
<input type="checkbox"/>	db-admin	NHI-6	SQL server administrator	it@leonardo-workshop.org	1
<input type="checkbox"/>	donatello	2	Donatello di Niccolo di Betto Bardi	donatello@leonardo-workshop.org	1
<input type="checkbox"/>	francis		King Francis I of France	king@kingdom.fr	1
<input type="checkbox"/>	hallway-scanner	NHI-5	Hallway scanner	scanner@leonardo-workshop.org	2
<input type="checkbox"/>	ldap-administrator	NHI-1	LDAP administrator	ldapadmin@leonardo-workshop.org	1

## What About Governance?

- Governance as an essence of managing NHI
- A high-level approach to NHI governance
- Why does NHI exist? (purpose)
- Who is responsible? (ownership)
- What can NHI do? (authorization)





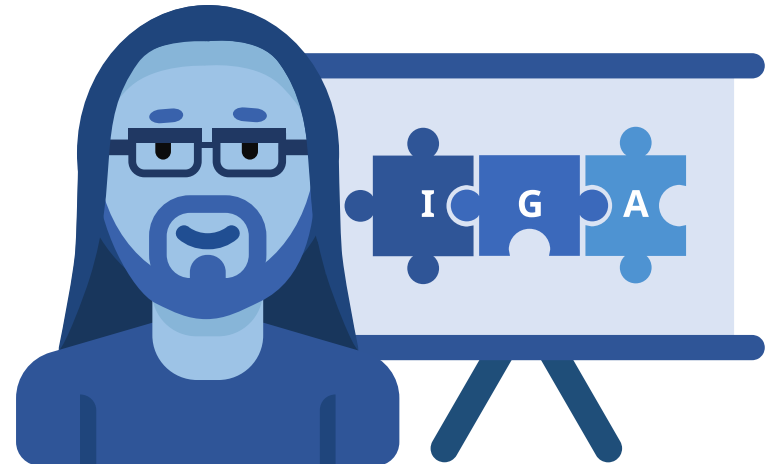
# Governance Principles Applicable to NHI

- Life-cycle management
- Approvals
- Access certifications
- Auditing
- Notifications
- Reporting
- Outlier detection
- Risk assessment



## Evolveum's View on NHI Governance

- Existing IGA principles are applicable to NHI
- Inventorization / catalogization
- Ownership management
  - React to ownership change
- Management using connectors
  - Expensive
  - Enables discovery, usage monitoring...
- Manage “master” identities for short lived ones
- Integration with specialized tools



## Conclusion

- Existing IGA principles are applicable to NHI
- You most likely have an IGA or IdM
- You can start by extending the existing IGA with NHI
  - Minimal initial investment
- Then you can continue with specialized tools or by extending NHI-related IGA processes
- **It is recommended to start with inventORIZATION & ownership responsibility**



# Thank you for your attention

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

Meet me and the Evolveum team at **booth #52**



/Evolveum



@Evolveum



/Evolveum



/Evolveum



/Evolveum

**Evolveum**

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