

# MAIA die KI im Zaum halten SoD Regeln und deren Ausnahmen UI Erweiterungen einfach und sicher

Geschäftsführer

**Martin Berndt**

OCG



Geschäftsführer

**Rüdiger Berndt**

OCG

# 01

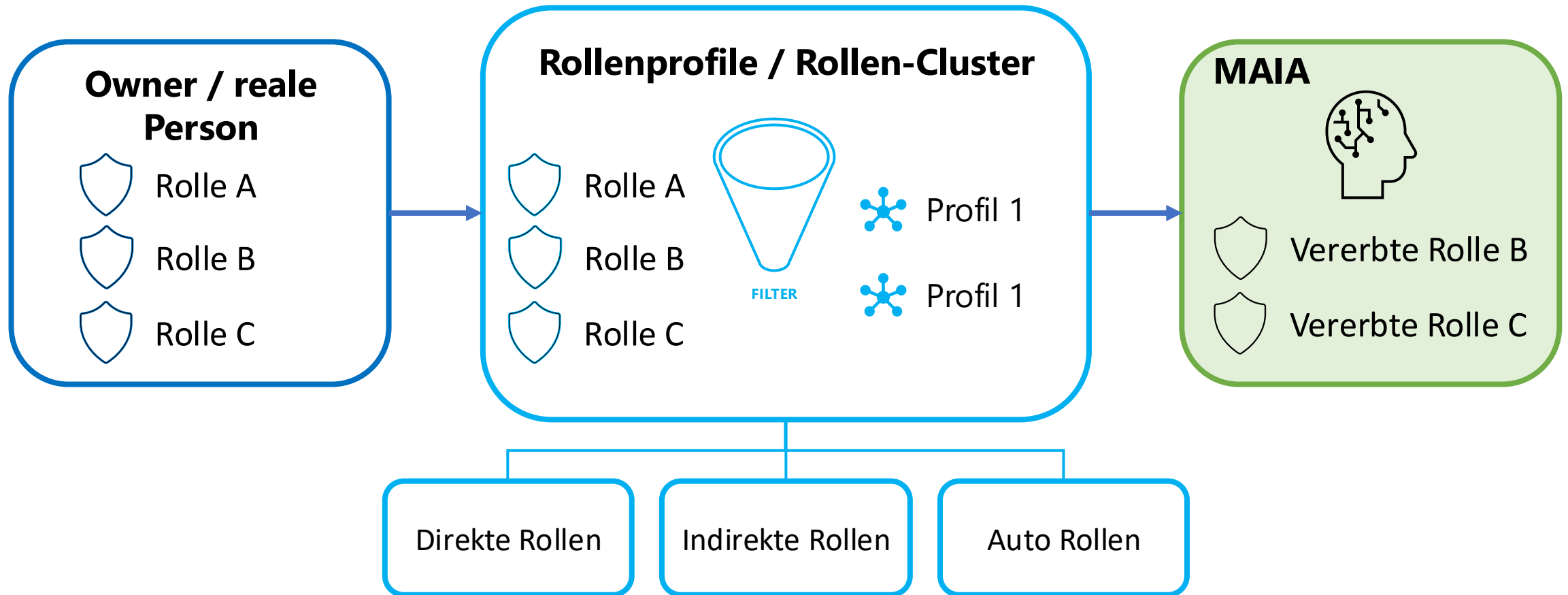
**MAIA – die KI im Zaum halten**



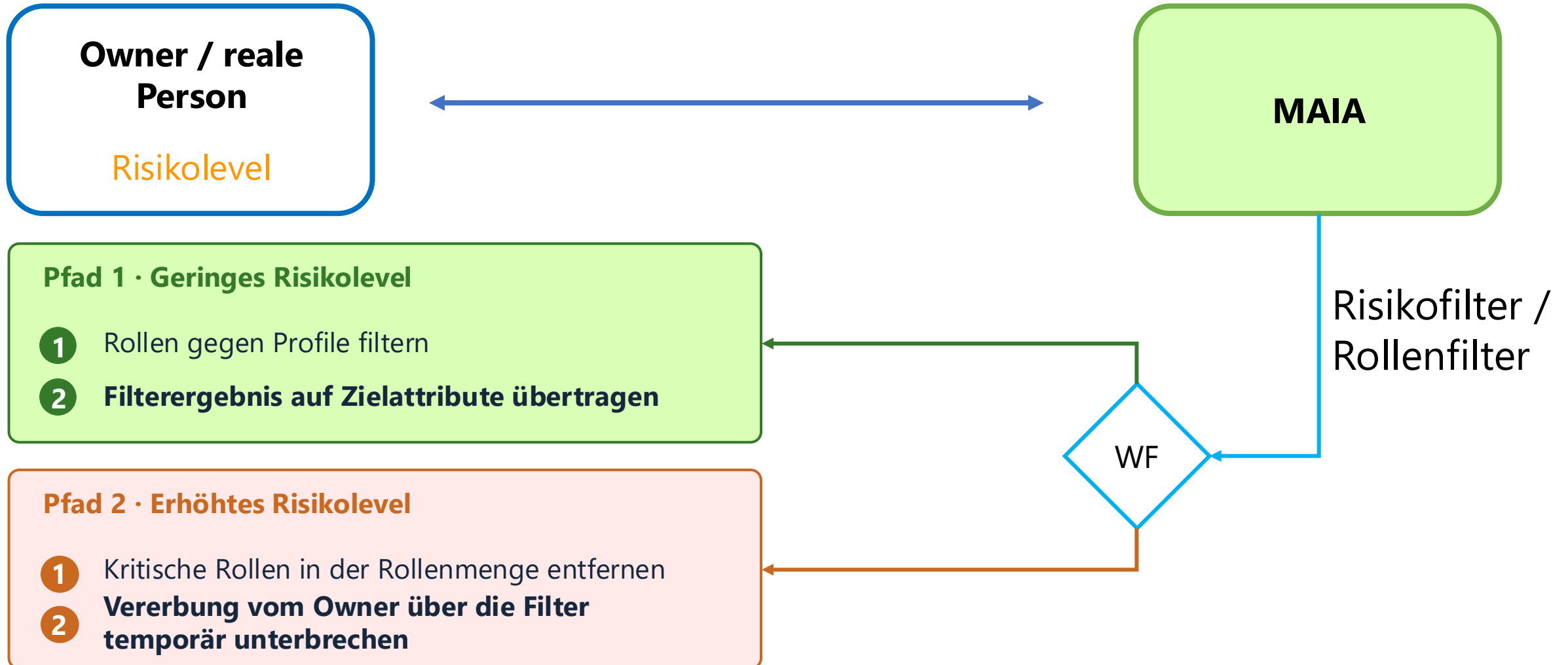
# FUNKTIONELLE ANFORDERUNGEN

- Eigene Identität für jede KI
- KI Agenten - Berechtigungen orientieren sich am „Eigentümer“
- Untermenge an Berechtigungen an MAIA „vererben“
  - Profilen der KI
  - Rollen des Eigentümers
- Risikolevel bestimmt Berechtigungen der KI
- Bei Deaktivierung des Eigentümers, auch Deaktivierung der MAIAs

# Least Privilege Prinzip für MAIAs



# Das Risikolevel steuert die Rollenvererbung



# 01

**LIVE DEMO**



# 02

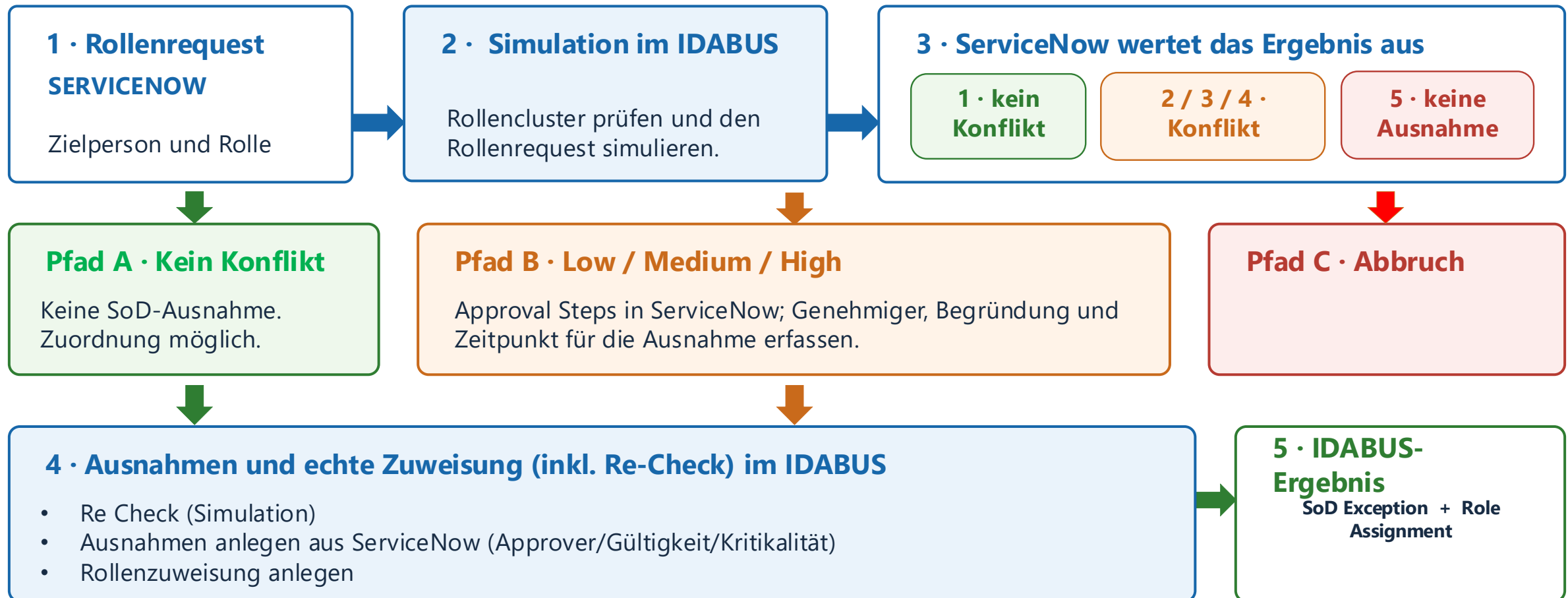
## SoD Regeln und Ausnahmen



# Funktionelle Anforderungen

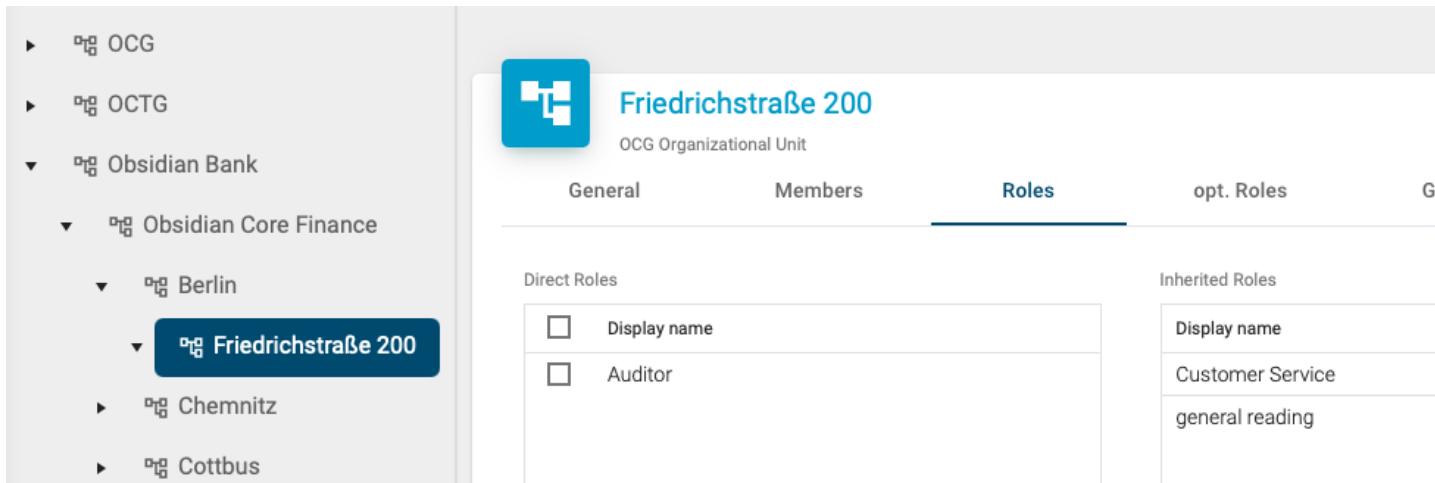
1. Rollen beantragen über über Self Services im Service Desk System (hier ServiceNow)
  1. Prüfung auf Konflikte gegen IDABUS SoD Regelbasis
  2. Ausnahmeprozesse im SNOW
  3. Auftrag an IDABUS über Zuordnung
2. Überprüfung der Verlängerung der Ausnahmen im IDABUS

# Simulieren > Genehmigen > Zuweisen

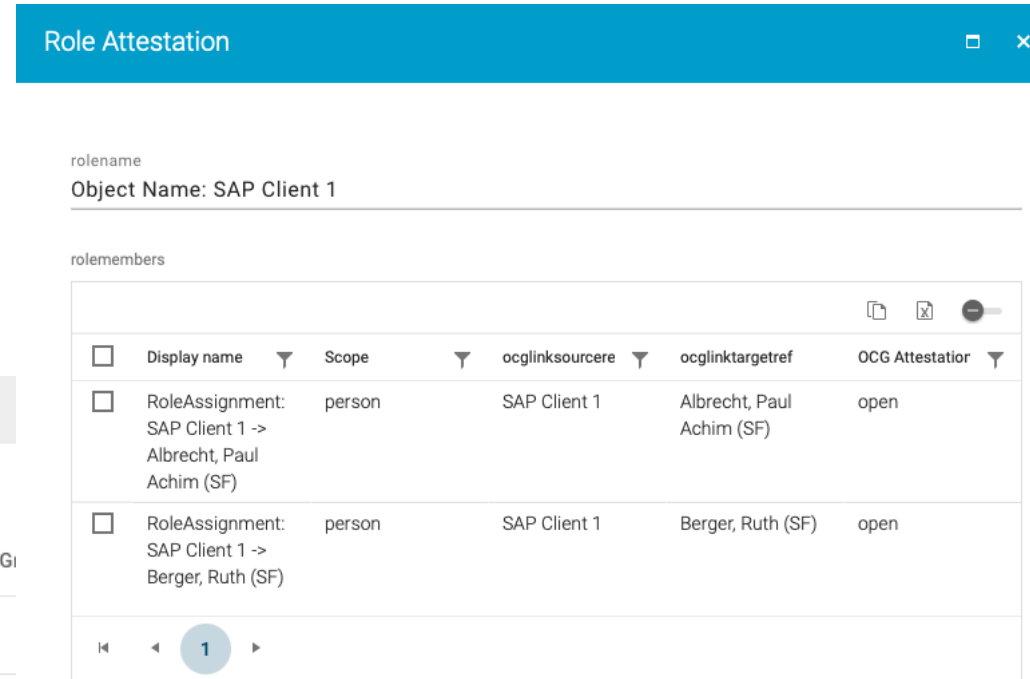


# Anschließende Prozessschritte

- **Report über durchgeführte Self Service Prozesse**
- **Attestierung der SOD Regeln, SOD Cluster, SOD Ausnahmen**
- **Manuelle Zuweisungen im IDABUS mit Approvals**
- **Rollenverwaltung über Organisationsstrukturen**



The screenshot shows the OCG organizational unit interface. On the left, a navigation tree lists organizational units: OCG, OCTG, Obsidian Bank, and Obsidian Core Finance. Under Obsidian Core Finance, there are three units: Berlin, Friedrichstraße 200 (highlighted), Chemnitz, and Cottbus. The main area displays the 'Friedrichstraße 200' unit, which is an OCG Organizational Unit. It has four tabs: General, Members, Roles (selected), and opt. Roles. The 'Roles' tab shows two columns: Direct Roles and Inherited Roles. Direct Roles include 'Display name' and 'Auditor'. Inherited Roles include 'Display name', 'Customer Service', and 'general reading'.



The screenshot shows the 'Role Attestation' window. It has a title bar with a close button. Below the title bar, there is a section for 'rolename' with the text 'Object Name: SAP Client 1'. Below this, there is a section for 'rolemembers' which contains a table of role assignments. The table has columns: Display name, Scope, ocglinksoucerc, ocglinktargetref, and OCG Attestation. There are two rows of data.

| Display name                                              | Scope  | ocglinksoucerc | ocglinktargetref          | OCG Attestation |
|-----------------------------------------------------------|--------|----------------|---------------------------|-----------------|
| RoleAssignment: SAP Client 1 -> Albrecht, Paul Achim (SF) | person | SAP Client 1   | Albrecht, Paul Achim (SF) | open            |
| RoleAssignment: SAP Client 1 -> Berger, Ruth (SF)         | person | SAP Client 1   | Berger, Ruth (SF)         | open            |

At the bottom of the table, there is a pagination bar showing '1' in a circle, indicating the first page of results.

## PATCH

**/api/v2/Workflow/execute/template/sync**

Executes the workflow with the given Id on the specified targets. Creates a request event even no targets exist. Does not create an event but fails if the inputParameters does not contain at least all required parameters of the workflow template or the user doesn't have permissions to execute the template.

## Parameters

Cancel

Reset

Name

Description

workflowTemplateId

string(\$uuid)

(query)

018c324f-86b7-4f52-a295-236a41395c27

comment

string

(query)

comment

SimulationSessionId

The ID of the simulation session.

string(\$uuid)

(query)

SimulationSessionId

SimulationActorId

An optional object ID of the simulated actor. The logged in user is taken if not specified.

string(\$uuid)

(query)

SimulationActorId

Request body required

application/json-patch+json

Edit Value | Schema

```
{
  "inputParameters": {
    "servicenowrequestid": "111",
    "targetpersonuniqueidentifier": "N000000000096834",
    "requestedroleuniqueidentifier": "N000000000105156"
  },
  "targets": [
```

## PATCH

**/api/v2/Workflow/execute/template/sync**

Executes the workflow with the given Id on the specified targets. Creates a request event even no targets exist. Does not create an event but fails if the inputParameters does not contain at least all required parameters of the workflow template or the user doesn't have permissions to execute the template.

## Parameters

Cancel

Reset

| Name                                             | Description                                                       |
|--------------------------------------------------|-------------------------------------------------------------------|
| workflowTemplateId<br>string(\$uuid)<br>(query)  | <input type="text" value="01893994-508d-418c-a1c7-9f929a4a313d"/> |
| comment<br>string<br>(query)                     | <input type="text" value="comment"/>                              |
| SimulationSessionId<br>string(\$uuid)<br>(query) | <input type="text" value="SimulationSessionId"/>                  |
| SimulationActorId<br>string(\$uuid)<br>(query)   | <input type="text" value="SimulationActorId"/>                    |

Request body required

Edit Value | Schema

```
{  
  "inputParameters": {  
    "servicenowrequestid": "111",  
    "targetpersonuniqueidentifier": "N000000000103270",  
    "requestedroleuniqueidentifier": "N000000000105164",  
    "criticality": "4",  
    "sodexceptionvaliduntil": "2026-09-03T22:00:00.000000Z",  
  }  
}
```



# 03

**UI-Erweiterungen – einfach und  
klar**

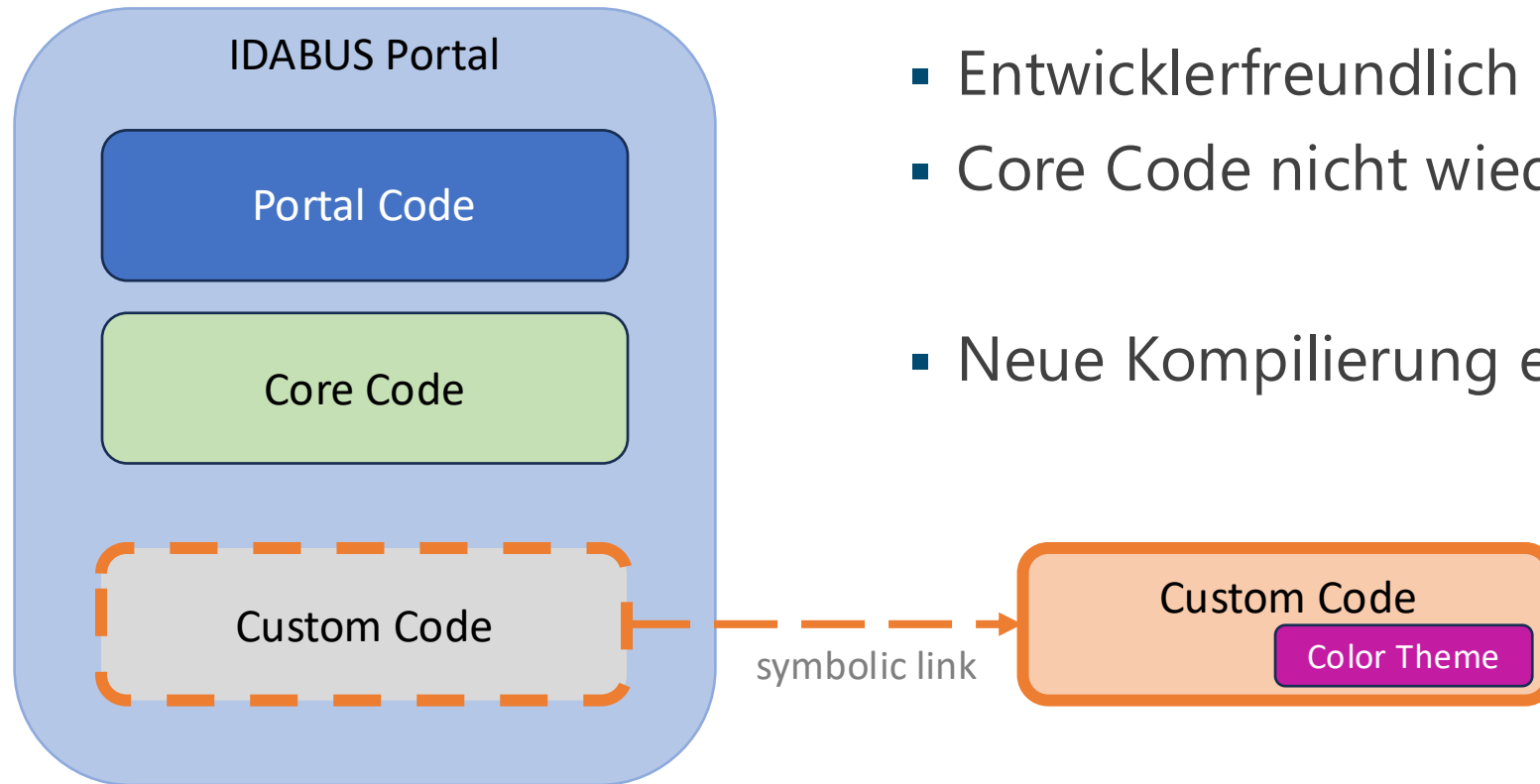


# Custom Code - Allgemein

- Umsetzung exakter Kundenwünsche
- Freie Gestaltung der UI



# Aktuell: Custom Code tief Integriert

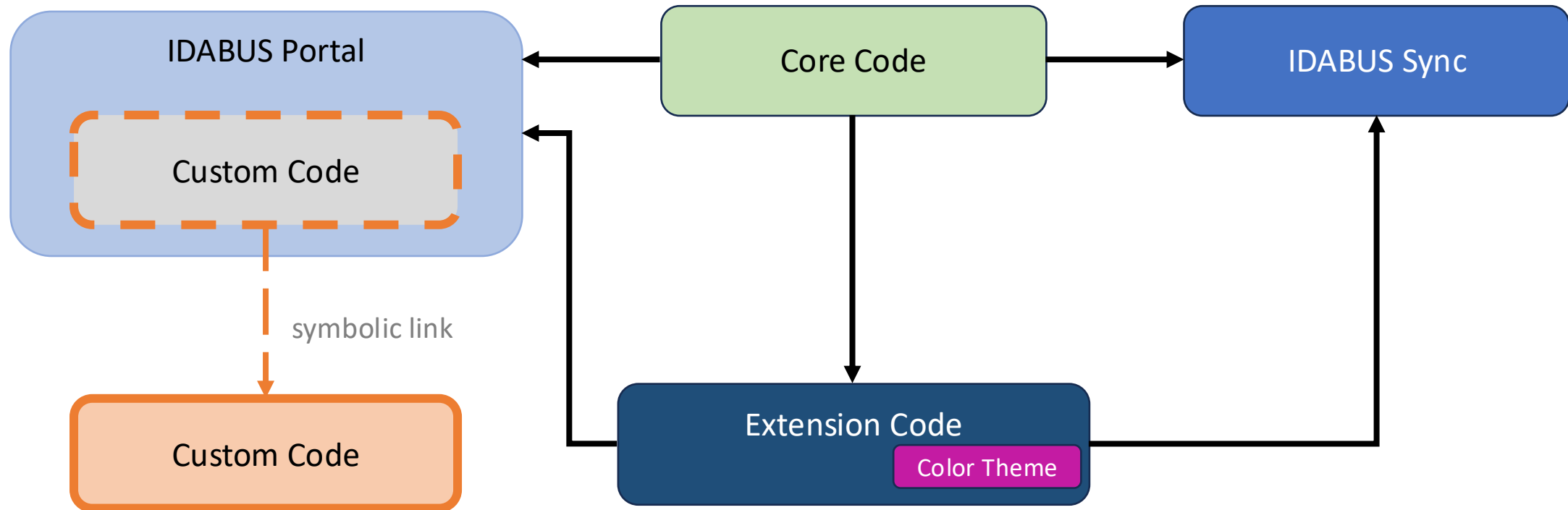


- Entwicklerfreundlich
- Core Code nicht wiederverwendbar
- Neue Kompilierung erforderlich

# Auswirkungen auf Updates



# Zukünftig: Trennung der Elemente



# Was wird besser?

Wiederverwendung

Core Code und Extension Code können als Bausteine wiederverwendet werden

Entwicklung im einzelnen Element

Extension Development braucht nicht mehr den Source Code des ganzen Projekts

Deployment ohne Rebuild

Änderungen können ohne neue Kompilation des Gesamtprojektes deployed werden

# Migration

- Custom Code bleibt kompatibel
- Bestehende Anpassungen werden 1:1 in Extensions überführt
- Keine fachliche Neuentwicklung nötig



# MAIAs, SoDs und Custom UI



UNIVERSITÄT ZU LÜBECK



# Zusammenfassung Summit 2026 & Ausblick

DANKE



UNIVERSITÄT ZU LÜBECK

