MidPoint Integrations: Partner Series

MidPoint and SCIM

How standards can help

Peter Gietz, 12 2024

CEO, DAASI International

Agenda

- Why Standards in Open Source
- Short Introduction into SCIM
- MidPoint and Self-Service
- MidPoint SCIM Connector

DAASI International

midPoint

Why Standards in Open Source

- OSS is not only about open source but also about interoperability and work division
  - No attempt to create golden cages
  - Rather it is important to interact with other products
- Reference implementations of standards are mostly if not always OSS
- In OSS clients and servers often are from different developers / vendors
- Open culture with open standards vs. closed source and proprietary protocols
  - Collaboration
  - Innovation and reference implementations
  - Standards conformity

SCIM

- Originally “Simple Cloud Identity Management”
  - thus designed as provisioning standard for the cloud
- Then renamed to “System for Cross-domain Identity Management”
  - Thus a generalisation for any provisioning between different domains
  - “the open API for managing identities”
  - JSON and RESTful based lightweight approach to identity provisioning
- Version 1.0 (December 2011), Version 1.1 (July 2012)
- Version 2.0 (September 2015)
  - Definitions, overview, concepts, and requirements: RFC7642
  - Core schema: RFC7643
  - Protocol: RFC7644

Extensions not (yet?) RFCs

- Active Internet-Drafts:
  - Device Schema Extensions to the SCIM model
    - Draft-ietf-scim-device-model-09, October 04, 2024
  - Cursor-based Pagination of SCIM Resource
    - Draft-ietf-scim-cursor-pagination-05, August 7, 2024
  - SCIM Profile for Security Event Tokens
    - Draft-ietf-scim-events-06 , June 6, 2024
  - SCIM Delta Query
    - Draft-sehgal-scim-delta-query-01 , July 8, 2024

Extensions not (yet?) RFCs

- Expired Drafts that might be revived again
  - Password and account status extensions for managing passwords and password usage
    - Draft-hunt-scim-password-mgmt-00, Expired: September 30, 2015
  - Just-in-time provisioning patterns in a protocol (such as SAML)
    - Draft-wahl-scim-jit-profile-02.txt, Expired: November 7, 2014
  - Privileged Access Management
    - Draft-grizzle-scim-pam-ext-01, Expired: April 21, 2018

SCIM Implementations

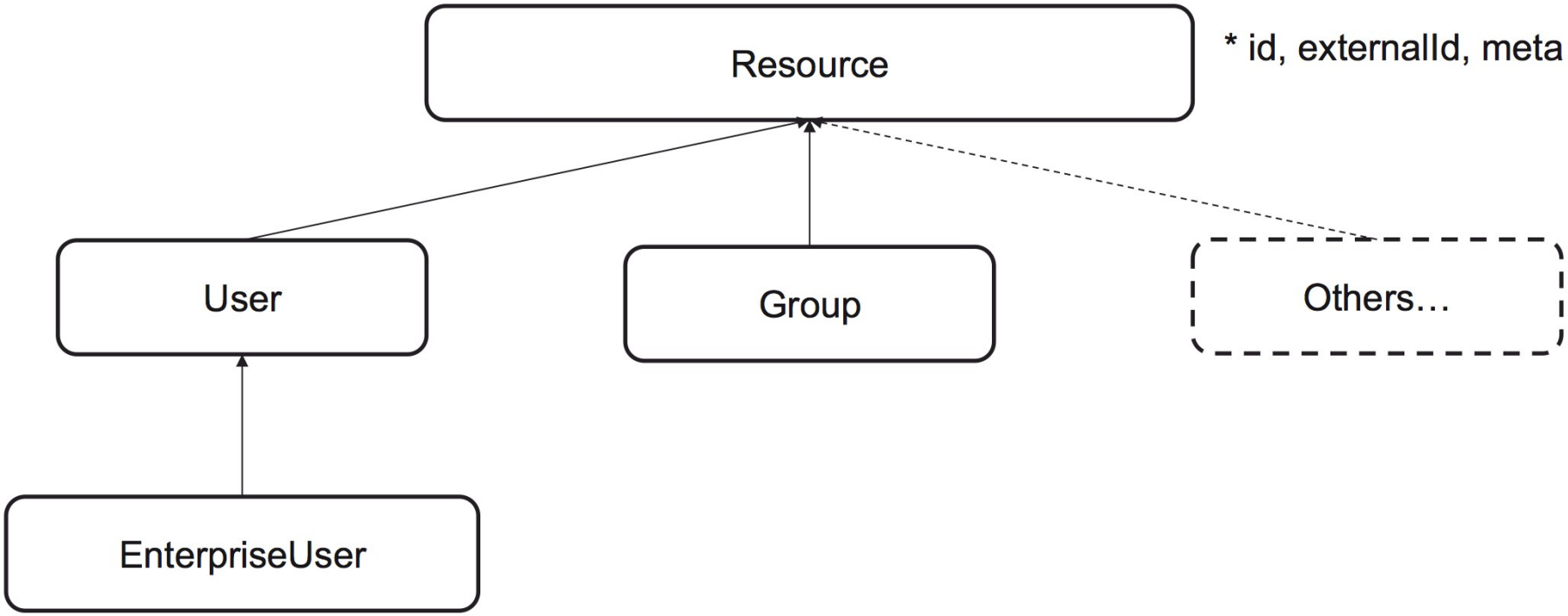
- http://www.simplecloud.info lists 45 implementations of SCIM 2.0 by e.g.:http://www.simplecloud.info lists 45 implementations of SCIM 2.0 by e.g.:
  - AWS SSO, Calendly, ConnId, Centrify, django-scim2, GitHub, Gluu, Microsoft Azure Active Directory and Entra ID*, NetIQ, Okta, Omada, One Identity, Oracle, Ping Identity, SailPoint, Salesforce, Syncope, UnboundID, WSO2, and many others
  - 22 are open source

*only outgoing

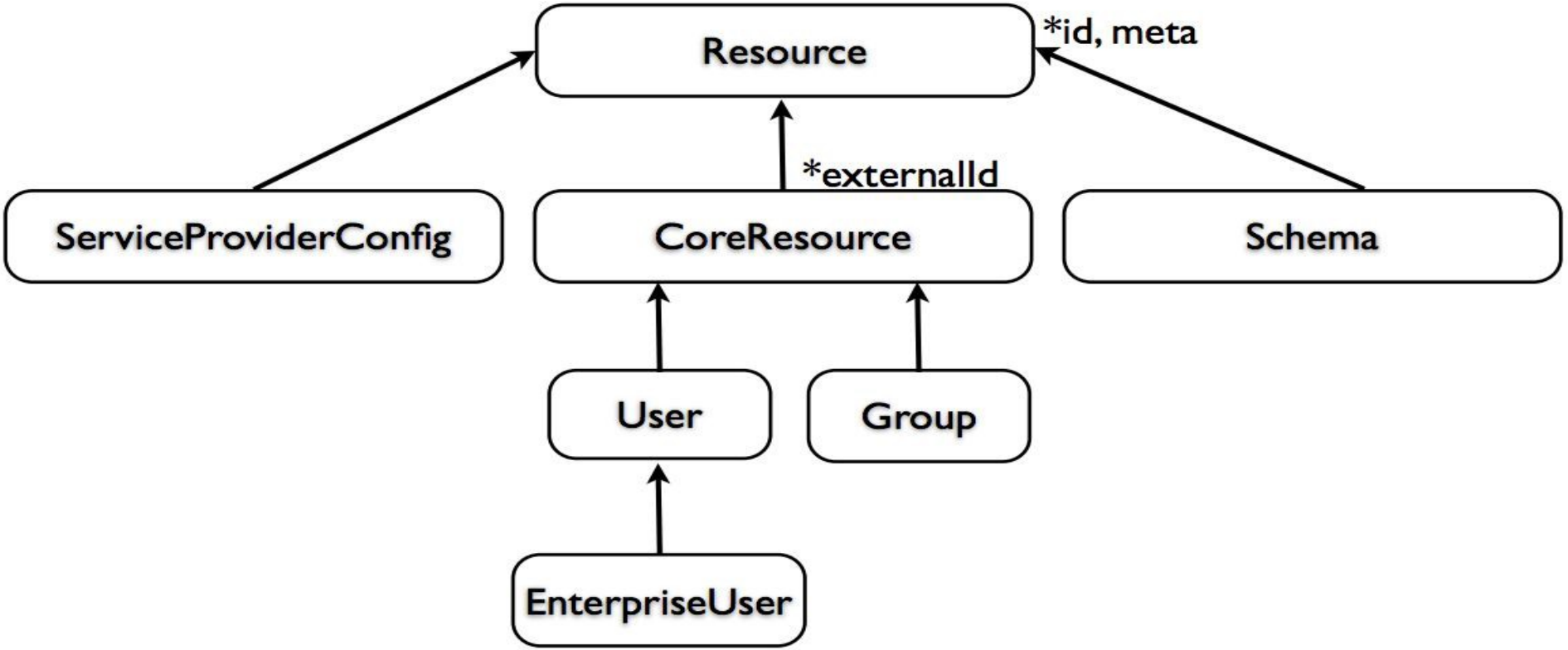
SCIM in a nutshell

- SCIM “is designed to manage user identity in cloud-based applications and services in a standardized way to enable interoperability, security, and scalability.” (RFC 7642)
- “SCIM's intent is to reduce the cost and complexity of user management operations by providing a common user schema, an extension model, and a service protocol” (RFC 7644)
- SCIM “provides a platform-neutral schema and extension model for representing users and groups and other resource types in JSON format. This schema is intended for exchange and use with cloud service providers.” (RFC 7643)
- “In essence: make it fast, cheap, and easy to move users in to, out of, and around the cloud.” (https://simplecloud.info)

SCIM Schema


Resource
* id, externalId, meta
User
Group
Others…
EnterpriseUser

SCIM Schema


Resource
*id, meta
*externalId
ServiceProviderConfig
CoreResource
Schema
User
Group
EnterpriseUser

Minimal representation of a user

```
{
  "schemas":      ["urn:scim:schemas:core:2.0:User"],
  "id": "2819c223-7f76-453a-919d-413861904646",
  "userName": "bjensen@example.com",
  "meta":
  {
    "resourceType": "User",
    "created": "2010-01-23T04:56:22Z",
    "lastModified": "2011-05-13T04:42:34Z",
    "version": "W\/\"3694e05e9dff590\"",
    "location":   "https://example.com/v2/Users/2819c223-7f76-
                   453a-919d-413861904646"
  }
}
```

user


```
{
  "schemas":  ["urn:ietf:params:scim:schemas:core:2.0:User"],
  "id": "2819c223-7f76-453a-919d-413861904646",
  "externalId": "701984",
  “meta”: {….}
  "userName": "bjensen@example.com",
  "name": {
    "formatted": "Ms. Barbara J Jensen, III",
    "familyName": "Jensen",
    "givenName": "Barbara",
    "middleName": "Jane",
    "honorificPrefix": "Ms.",
    "honorificSuffix": "III"     },
  "phoneNumbers":[ { "value":"555-555-8377", "type":"work" } ],
  "emails":[ {
      "value":"dschrute@example.com",
      "type":"work",
      "primary": true  }
}
```

Standardised extension enterprise user

```
{
  "schemas":["urn:ietf:params:scim:schemas:core:2.0:User",
“urn:ietf:params:scim:schemas:extension:enterprise:2.0:User
"],
  "id": "2819c223-7f76-453a-919d-413861904646",
  ...
  “employeeNumber”: { “value“: “xxx” } ,
  “costCenter”: { “value“: “xxx” } ,
  “organization”: { “value“: “xxx” } ,
  “division”: { “value“: “xxx” } ,
  “department”: { “value“: “xxx” } ,
  “manager”: { “value“: “xxx” } ,
...
```

More extensions are possible

- Already 2013 we spoke about SCIM schema for eduPerson [1]
- Recently there was some talk about SCIM schema for eduPerson and voPerson in the frame of AARC Tree [2]
  - If overly busy people find time for it, that might happen
  - Breaking news: a new task force has been created to do this work
- DAASI International already extended the schema for Role information

[1] See https://tiimeworkshop.eu/proceedings/2020/sessions/session33/
[2] See https://aarc-community.org/aarc-tree-project/

DAASI (yet proprietary) Extensions

- Motivation
  - add additional Resource Types, i.e. Roles
  - include meta information, i.e. permissions from PDP, or lastLogin
  - include customer specific attributes
- How extended
  - schema extensions: we try to stick as close as possible to the standard SCIM specifications. i.e. Roles are analogue to Groups.
  - protocol extensions: i.e. additional parameters to support multi tenancy.

DAASI International

midPoint

DAASI (yet proprietary) Extensions

- How it works in practice
  - GET /User returns additional JSON attributes such as "tenant" or "roles"
  - GET /Groups?local_search=true only returns groups from tenant of authenticated user.
    - In particular: if tenant is root-tenant, do not include Groups from subtenants

Critics of SCIM

- Evolveum[1] sees a number of issues in SCIM:
  - More than one way to represent names
  - Concept of group with members, can lead to very big groups (just like in LDAP)
  - Mandatory unique user name might be problematic in create operations where the target service needs to ensure uniqueness
  - “As long as you are aware of all the limitations of SCIM and it still satisfies your needs it is perhaps OK to use SCIM.”
- I would say: Yes one should be aware of potential limitations, but: if there is a standard, use it
  - For completeness
  - For interoperability

[1] See https://docs.evolveum.com/midpoint/devel/design/scim-troubles/

SCIM and midPoint

- “We do not use SCIM in midPoint, not directly anyway”[1]
- midPoint “API is much richer than SCIM”
- “even though the schemas are similar, they are not the same” and “not directly compatible”
- “MidPoint supports SCIM indirectly.
  - There are a couple of SCIM-based connectors for some services.
  - And we expect that we will develop more such connectors in the future
  - There are efforts to create a SCIM API for midPoint as a contribution to midPoint project. (I assume that this refers to our SCIM Overlay, see below)

[1] See https://docs.evolveum.com/midpoint/devel/design/scim-troubles/

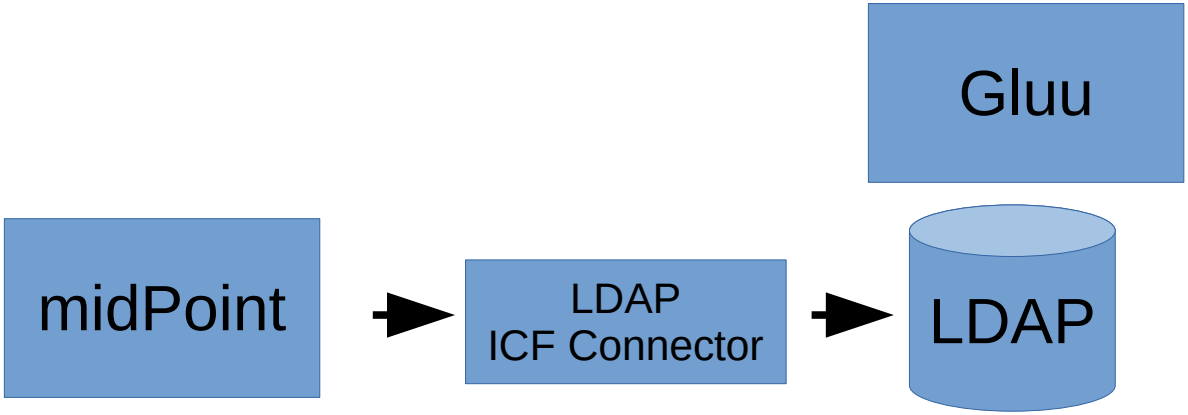
SCIM Connectors for midPoint

- SCIMv1 Generic Connector [1]
  - Implements SCIM 1.1 (from Evolveum)
- SCIMv1 Salesforce Connector [2]
  - for Salesforce platform using SCIM 1.1 API (same source)
- SCIM v1 Slack connector [3]
  - for Slack using SCIM 1.1 API (same source)
- SCIM2 Connector [4]
  - for SCIM2 compatible systems (from Exclamationlabs, now Provision IAM)
- GLUU SCIM Connector [5]
  - for GLUU server based on SCIM (from DAASI International)

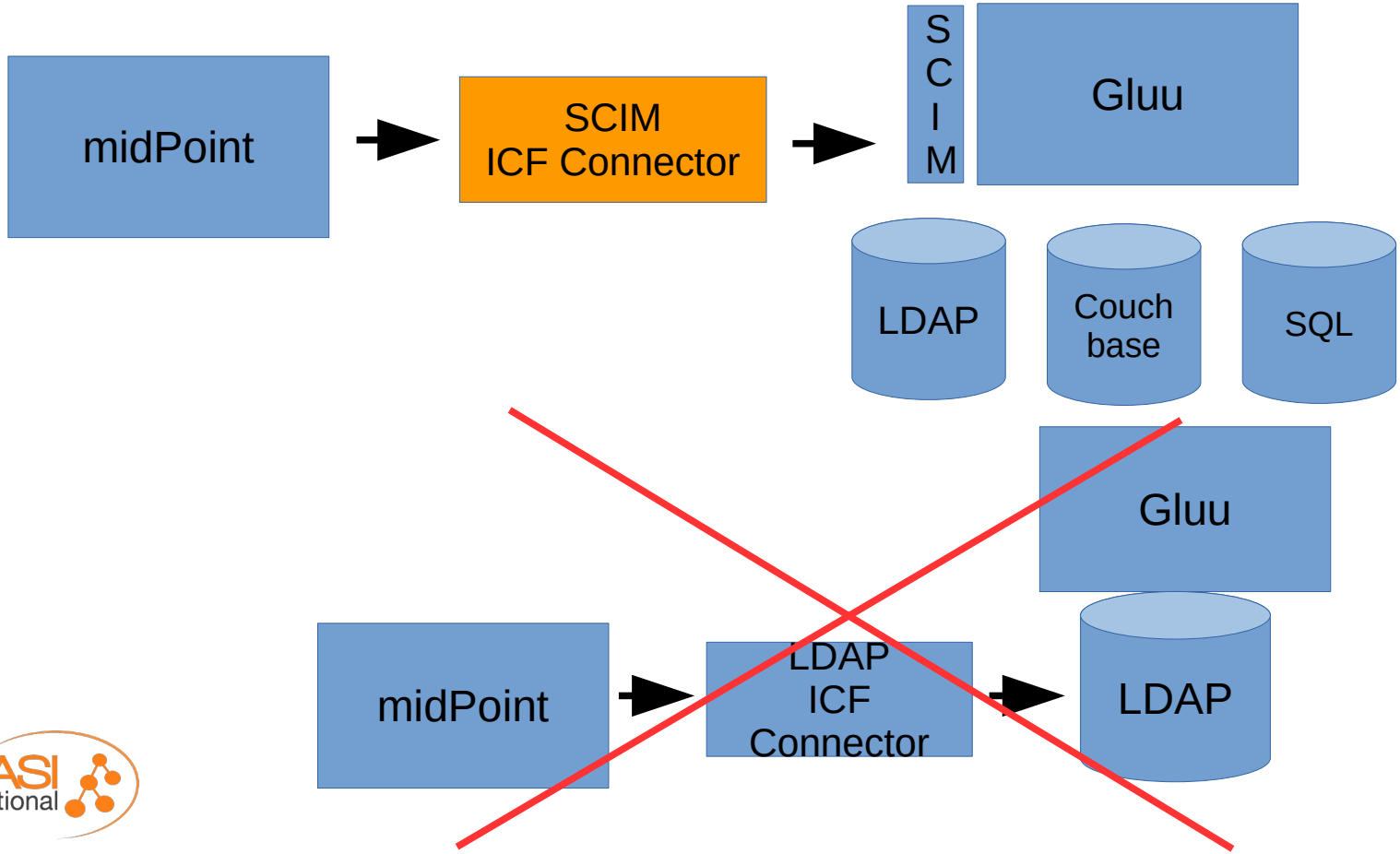
[1] https://github.com/Evolveum/connector-scim1
[2] https://github.com/Evolveum/connector-scim1
[3] https://github.com/Evolveum/connector-scim1
[4] https://github.com/ExclamationLabs/connector-scim2
[5] https://gitlab.daasi.de/midpoint/midpoint-gluu-client/

DAASI International

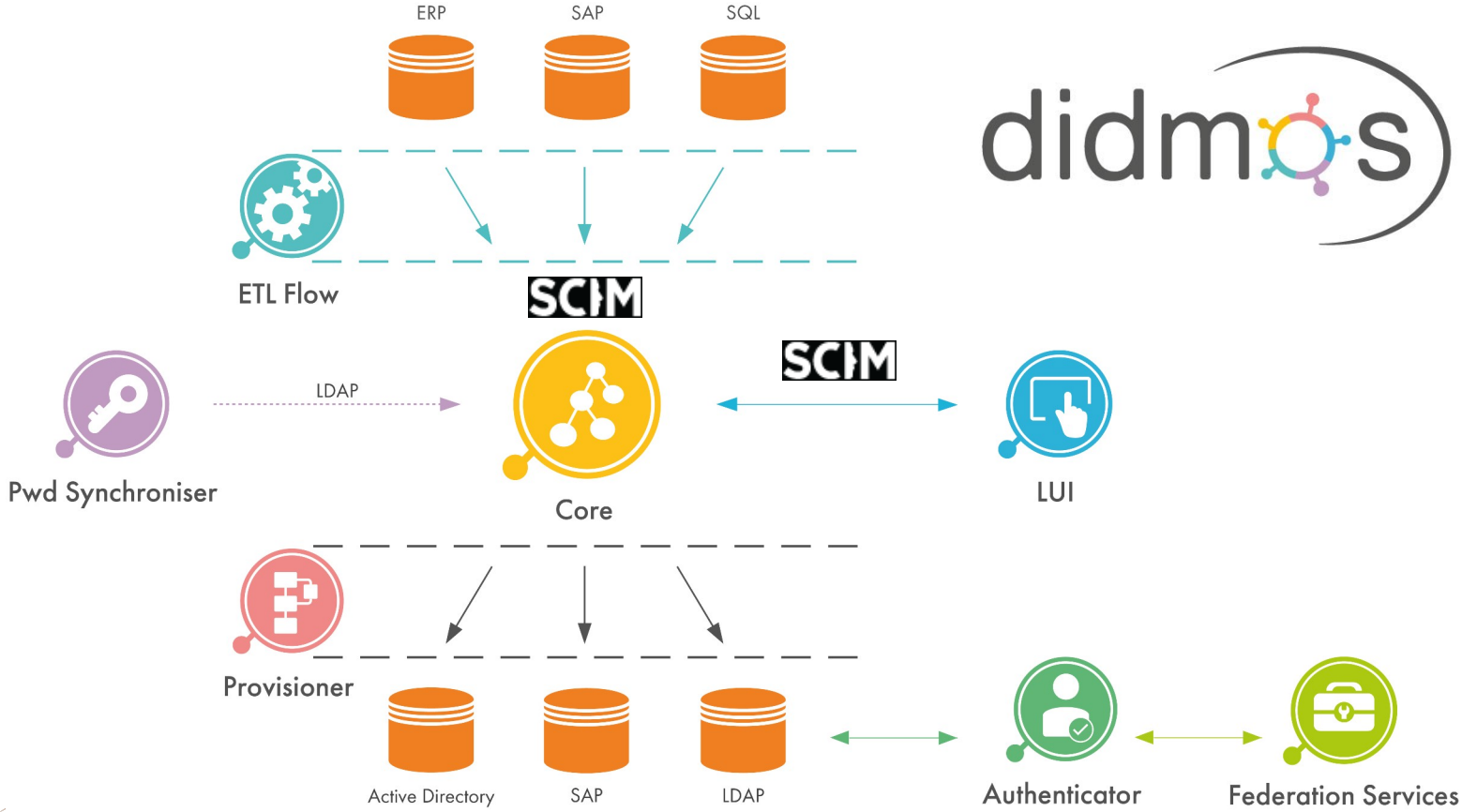
Usecase MidPoint and Gluu: without SCIM



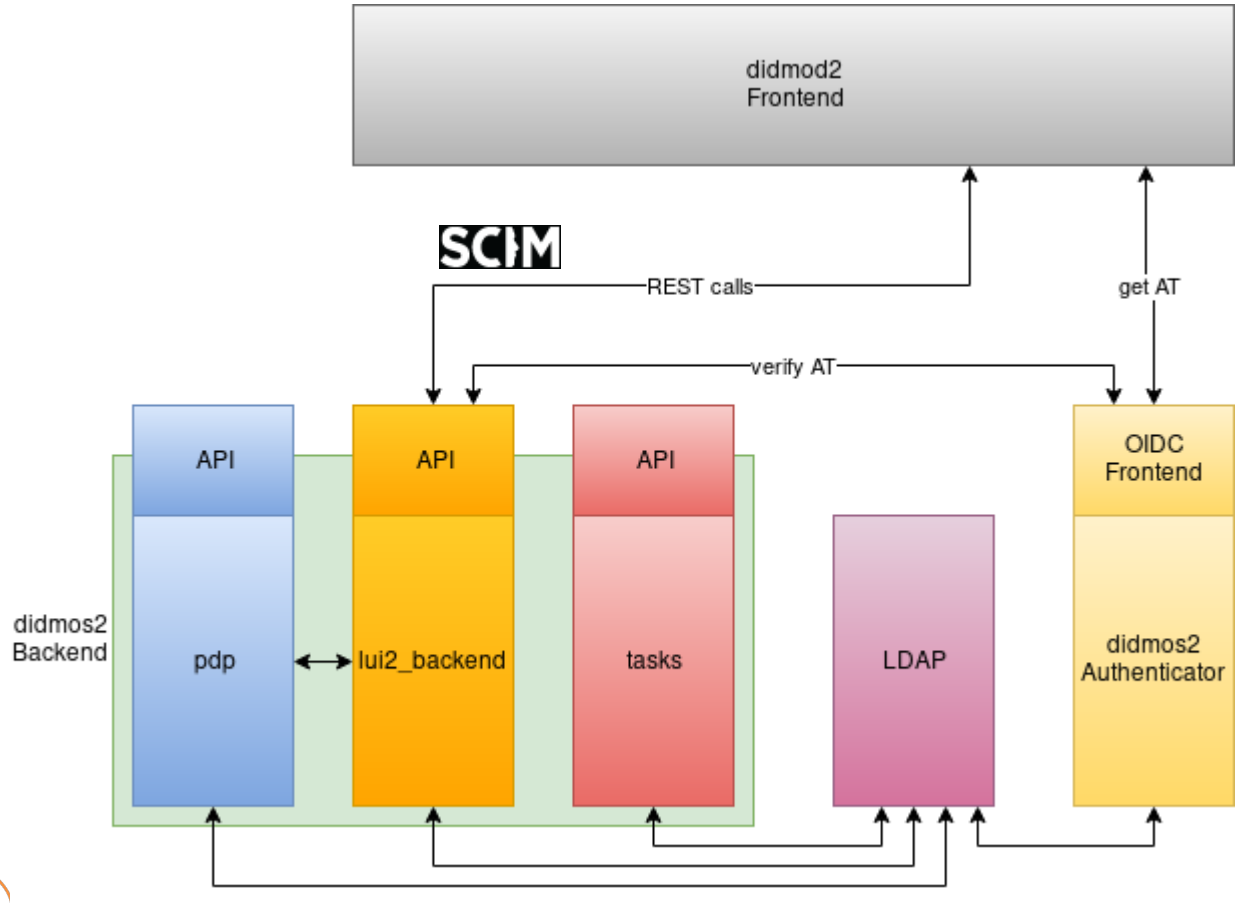
MidPoint and Gluu via SCIM



DAASI's didmos uses SCIM internally



DAASI's didmos uses SCIM internally



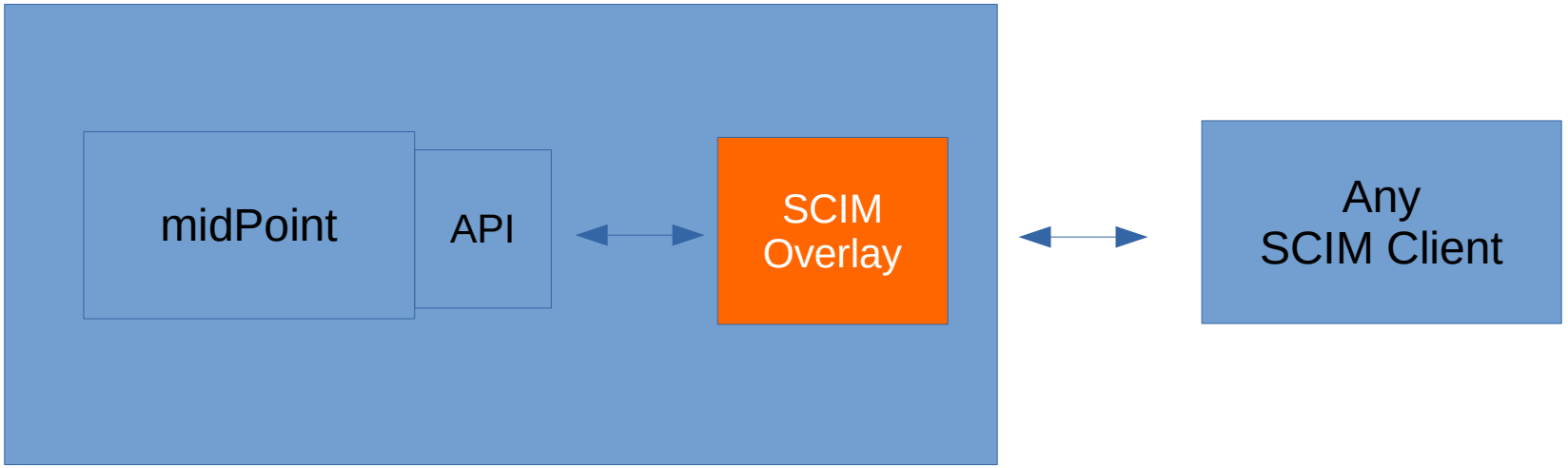
How to enable SCIM in midPoint

- DAASI had a customer that wanted to interact with midPoint via SCIM
  - To integrate their own API-Gateway that supported SCIM
  - To add an own frontend that should also be reusable elsewhere
- Thus we developed a SCIM-Overlay in midPoint
  - Code available at https://gitlab.daasi.de/midpoint/midpoint-scim-overlay

LUI Frontend for midPoint Selfservice

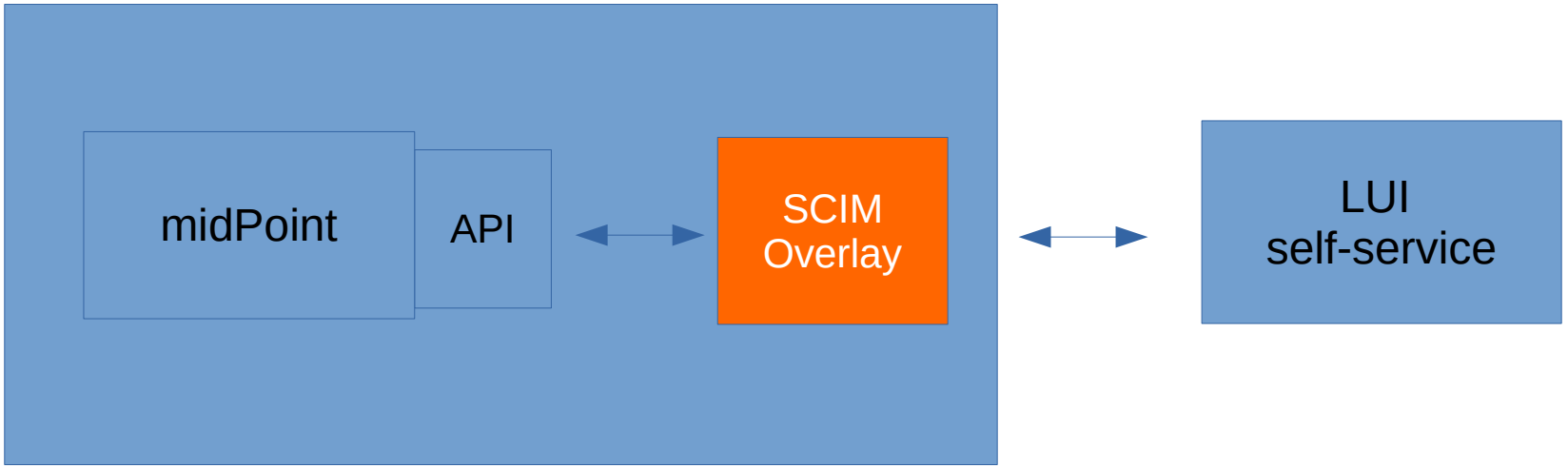
- Having the Open Source SCIM Overlay and our LUI-based self-service, we now have a good solution for a midPoint self-service that is:
  - highly configurable
  - flexibly extensible and
  - adjustable to customer corporate design

MidPoint SCIM Overlay



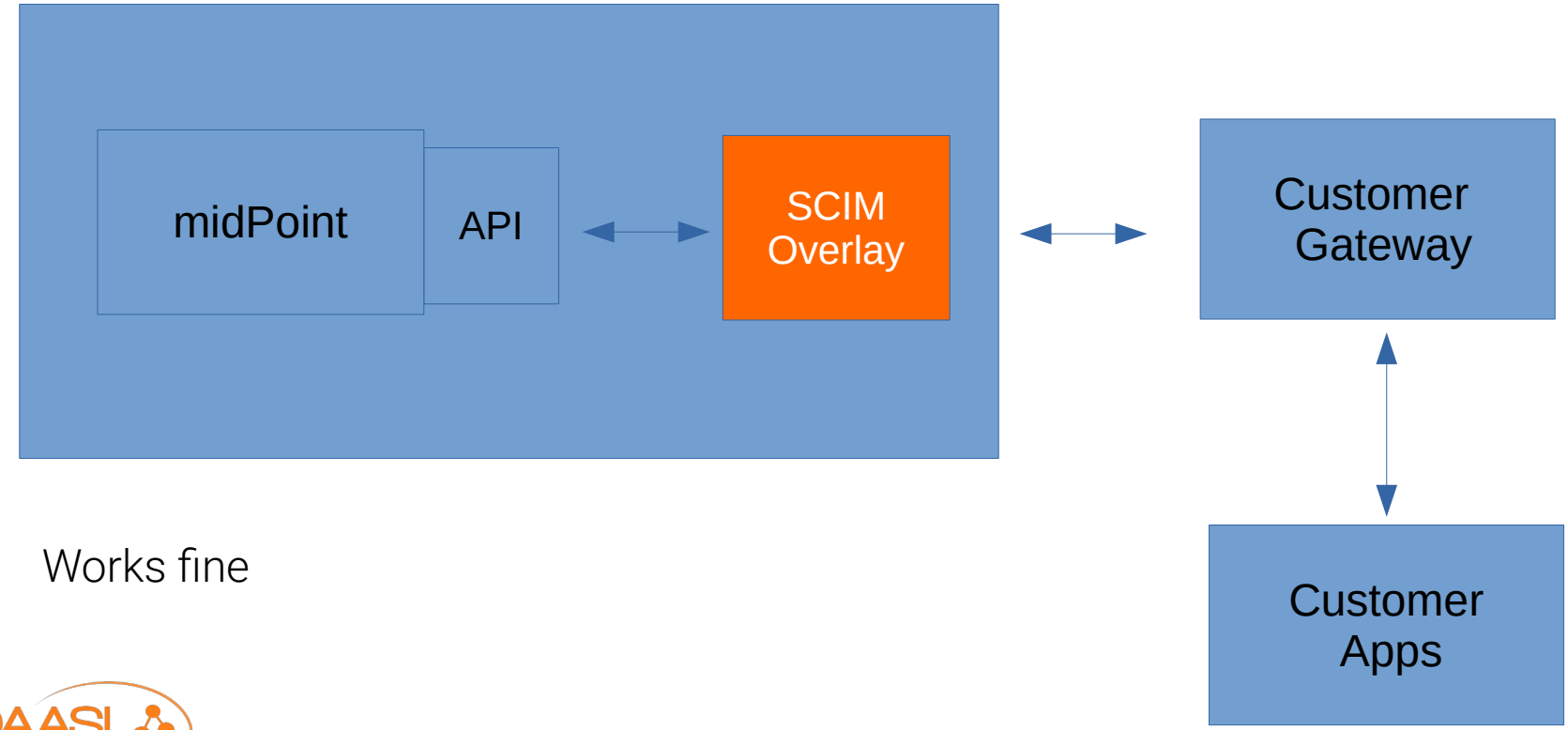
May be with some adjustments in the overlay

MidPoint SCIM Overlay



Works fine

MidPoint SCIM Overlay



Works fine

SCIM: a lingua franca?

- SCIM is supported by many vendors and developers
- SCIM has an extension mechanism
  - Different schema, same REST protocol
- In didmos2 we defined some internal extensions
  - Could be standardized
- SCIM can be used to integrate different open source products
- SCIM and midPoint is a good fit (as far as we are concerned)
  - Connectors
  - Overlay
- Of course the mentioned limitations need to be taken into account

DAASI International

Thanks for listening!

Questions?

See https://app.sli.do/event/r6RPXHiyU7cs5L67AxmQRq/live/questions

Thank you for your attention

Phone: +49 7071 407109-0

Email: info@daasi.de

Web: www.daasi.de