Reg-app

https://git.scc.kit.edu/reg-app

also https://github.com/cyber-simon/reg-app (pull requests)

and https://hub.docker.com/r/cybersimon/reg-app (docker images)

Basics

- Application based on JEE8
  - MVC based development
  - Transaction management on service layer
- Libaries in use
  - JPA ORM
  - OpenSAML
  - Nimbus SDK (OIDC)
  - Primefaces
  - Omnifaces
  - Drools
  - Bouncycastle
- Tested and developed on Wildfly
- Published under GPLv3

Timeline

- Development started 2012
- In production use since 2013
- Extension of functionality since then
  - New requirements
- Future plans
  - Migrate Backend/ Service layer to Quarkus
    - All service function as RestAPI accessible with access token
  - Develop Single Page App for Client functions

SAML

- Act as SAML SP
  - Use multiple federation metadata
  - Filter federation metadata with entity categories or drools
  - Keyrollover (primary/secondary Certificate/Key)
  - Use scripting and hooks based on IDP
  - Issue AttributeQuery to home IDP
    - TLS and XmlDSig authentication
    - Based on service usage (Rest API for services)
    - Based on attribute freshness interval
- Act as SAML IDP
  - Use SPs from federation metadata
  - Add SPs directly
  - Configure released attributes via script
  - Optionally connect SP to one or more services
  - Require 2fa based on SP atm/ script based in near future

OIDC

- Act as OIDC RP
  - Manual configuration atm
  - OIDC federation in the future?
  - Support in Nimbus SDK seems to be there: https://connect2id.com/products/nimbus-oauth-openid-connect-sdk/examples/openid-connect/federation
  - User update via refresh token
    - Based on service usage (Rest API for services)
    - Based on attribute freshness interval
  - Use scripting and hooks for data manipulation per OP
  - Primary/secondary Certificate/Key for rollover
- Act as OIDC OP
  - Configure released claims via script
  - Configure token format per RP (token lifetime, refresh token extendable, …)
  - Optionally connect RP to one or more services
  - Optionally check access rule
  - Require 2fa based on RP atm/ script based in near future
- Future Plans
  - Extend OIDC to be more feature complete
  - OIDC Token Exchange

Tested against

- SAML SP
  - Shibboleth IDP
  - SimpleSamlPhp
  - CAS IDP
- SAML IDP
  - Shibboleth SP
  - Nextcloud
- OIDC RP
  - Keycloak
  - Unity
  - Google
  - Orcid
  - LS AAI
  - Academic Cloud
- OIDC OP
  - Nextcloud
  - Apache2 mod-auth_openidc
  - Quarkus Rest OIDC with SPA

2FA

- Modular 2FA interface
  - Yet supported token types
    - TOTP (Hardware/software)
    - HOTP Tan List (LinOTP)
    - Paper Tan List (PrivacyIDEA)
    - Yubikey OTP
- Modules
  - LinOTP: productive sind 3 years
  - PrivacyIDEA: tested, not yet used in production, but very similar to LinOTP
- Script-based decision for 2FA configuration
  - i.e. different 2FA server can be used for users from different home orgs
  - Visibility level can be configured
    - Token manageable
    - Only readable
    - Only for validation

User lifecycle

- Trigger AttributeQuery or Token Refresh based on last user update
- If AttributeQuery answer is Unknown Principal, set users status „on_hold“
- Same for OIDC Token refresh
  - Test cases and prodction experience not yet on the same level
- After configurable amount of time, scrub all personal data from user
  - Keep the pairwaise or persistent ID and interal uidNumber yet
- After more time (configurable) also drop persistent/pairwise ID and uidNumber
- Future plan: Inform user to login, after some time, if attributes can not be refreshed

Service provisioning

- User can register for services
- Service provisioning modular and configurable per service
- Implemented service modules
  - LDAP
    - Provision user data in LDAP Server
    - Attribute names and values per velocity template of script
    - Group capable
  - Nextcloud
    - Different flavors (full user management, on the fly creation)
  - Openstack
- Access rules per service
- Use policies per service
- User can deregister from service
- Users can be automatically deregistered from a service
  - Base on users status (i.e. on_hold or lost_access) and status change time

Rolemanagement

- Roles can include users and groups
- Rolemodel for managing different aspects
- Hardcoded roles for admin interface
  - RoleAdmin, ServiceAdmin, SamlAdmin, OidcAdmin, UserAdmin, BusinessRuleAdmin, TemplateAdmin, RestAdmin, TimerAdmin,…
  - Created on the fly on application start
- Roles for services
  - Admin for service: manages users who registered for the service
  - Groupadmin for service: manages groups for a service

Groups

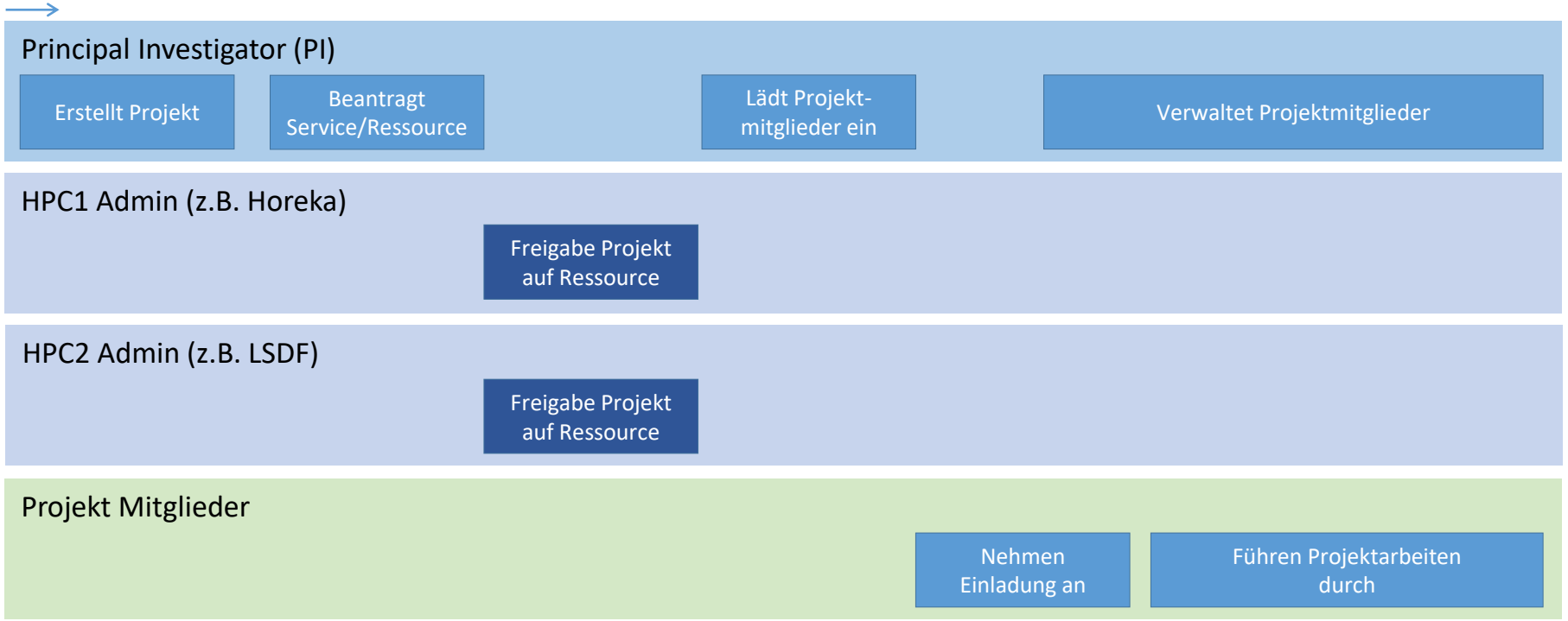
- Local groups
  - Standard case: Local group is for a specific service
  - Can also be conneccted to other services read-only
  - Are managed locally by group admin
- Groups from home organisation
  - Generated based on attribute or claims
  - Connected to the home IDP or OP
- Attribute sourced groups
  - Depend on a attribute source

Attribute sources

- Bound to speicific service
- For all users
- Attribute sources are queried on user updates
- Modular interface
- Currently one modules: HttpAttributeSource
- Issues a Http request and can process JSON or plain text result
- Attribute source query results are stored with the user object and can be used in access rules or register modules

Community/Project/VO Management

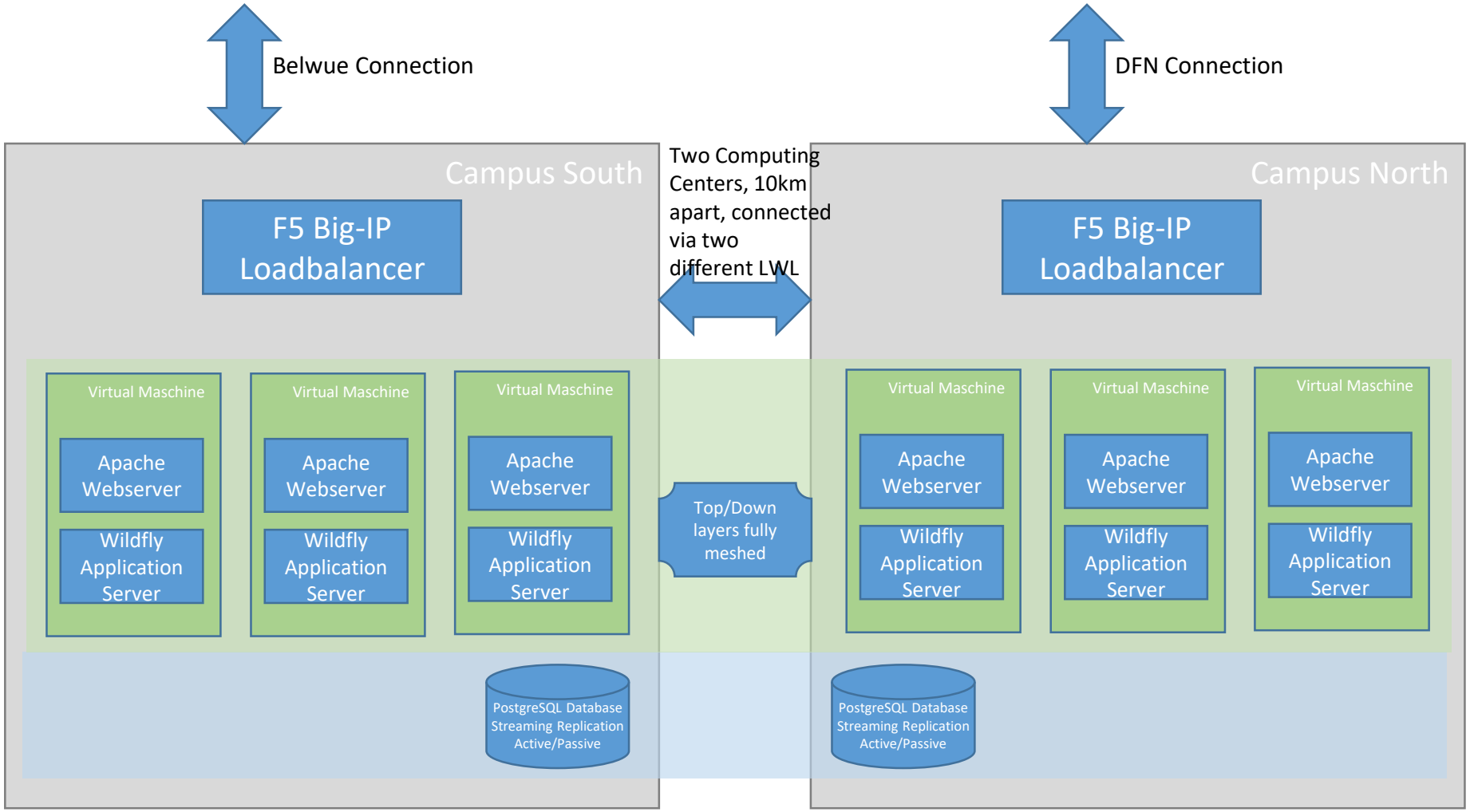
- In development
- The process is currently reviewed by our HPC and legal department
- Projects can be used by services, or send as claims or attributes
- Like groups from home orgs, projects can be created on claims, attributes from other sources (IDP, OP or attribute source)



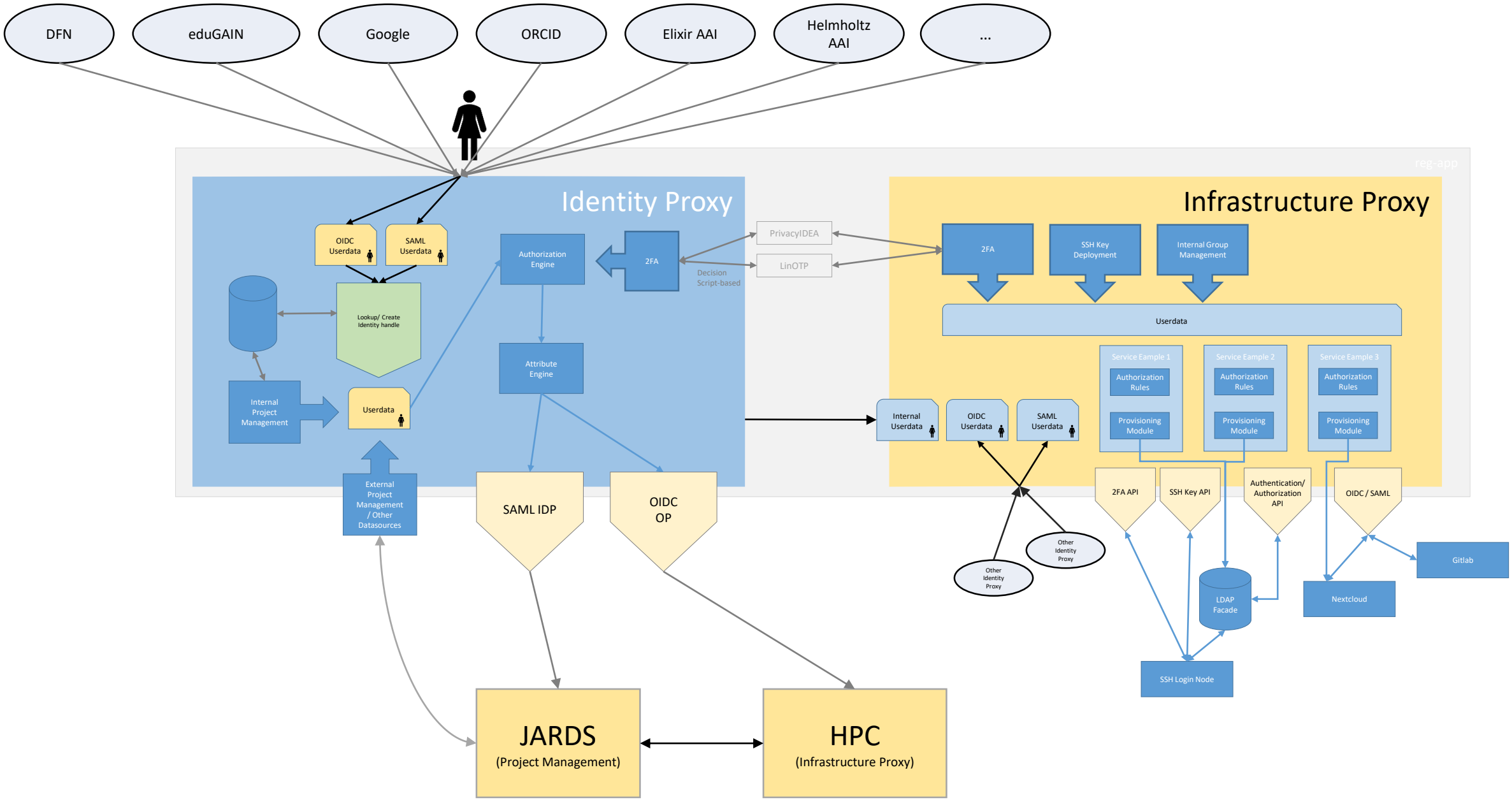
Webinterface

- Can be customized…
  - Completly at compile time, by exchanging the templates mentioned in the POM file
  - Simply at runtime, by providing own CSS files, some links and images
  - Completly at runtime, by replacing xhtml files, which can also be loaded from DB
- Virtual Hosts
  - Runtime customization of look and feel, can be defined per host

Production Env at KIT



- 53k active users
- 27k deprovisioned users


DFN
eduGAIN
Google
ORCID
Elixir AAI
Helmholtz AAI
...
reg-app
Identity Proxy
OIDC Userdata
SAML Userdata
Authorization Engine
2FA
PrivacyIDEA
LinOTP
Decision Script-based
Lookup/ Create Identity handle
Attribute Engine
Internal Project Management
Userdata
External Project Management / Other Datasources
SAML IDP
OIDC OP
Infrastructure Proxy
2FA
SSH Key Deployment
Internal Group Management
Userdata
Service Eample 1
Service Eample 2
Service Eample 3
Authorization Rules
Provisioning Module
Internal Userdata
OIDC Userdata
SAML Userdata
2FA API
SSH Key API
Authentication/ Authorization API
OIDC / SAML
Other Identity Proxy
Other Identity Proxy
LDAP Facade
Gitlab
Nextcloud
SSH Login Node
JARDS
(Project Management)
HPC
(Infrastructure Proxy)