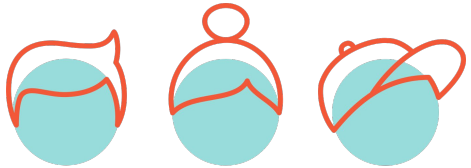
Technical introduction

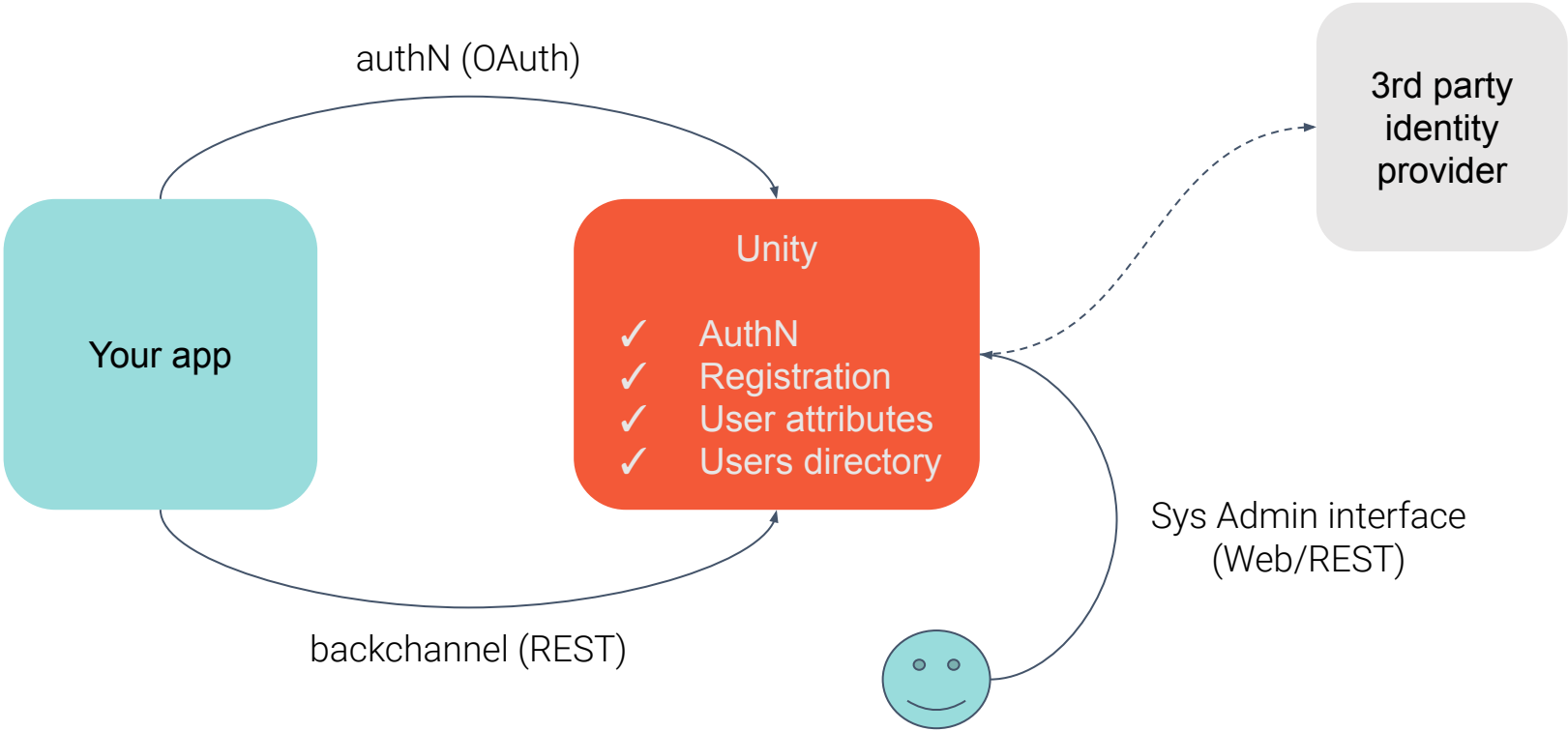
NFDI AAI meeting, 18.08.2022



Outline

- Application areas
- Unity ecosystem
- Technical overview
- Relevant companion

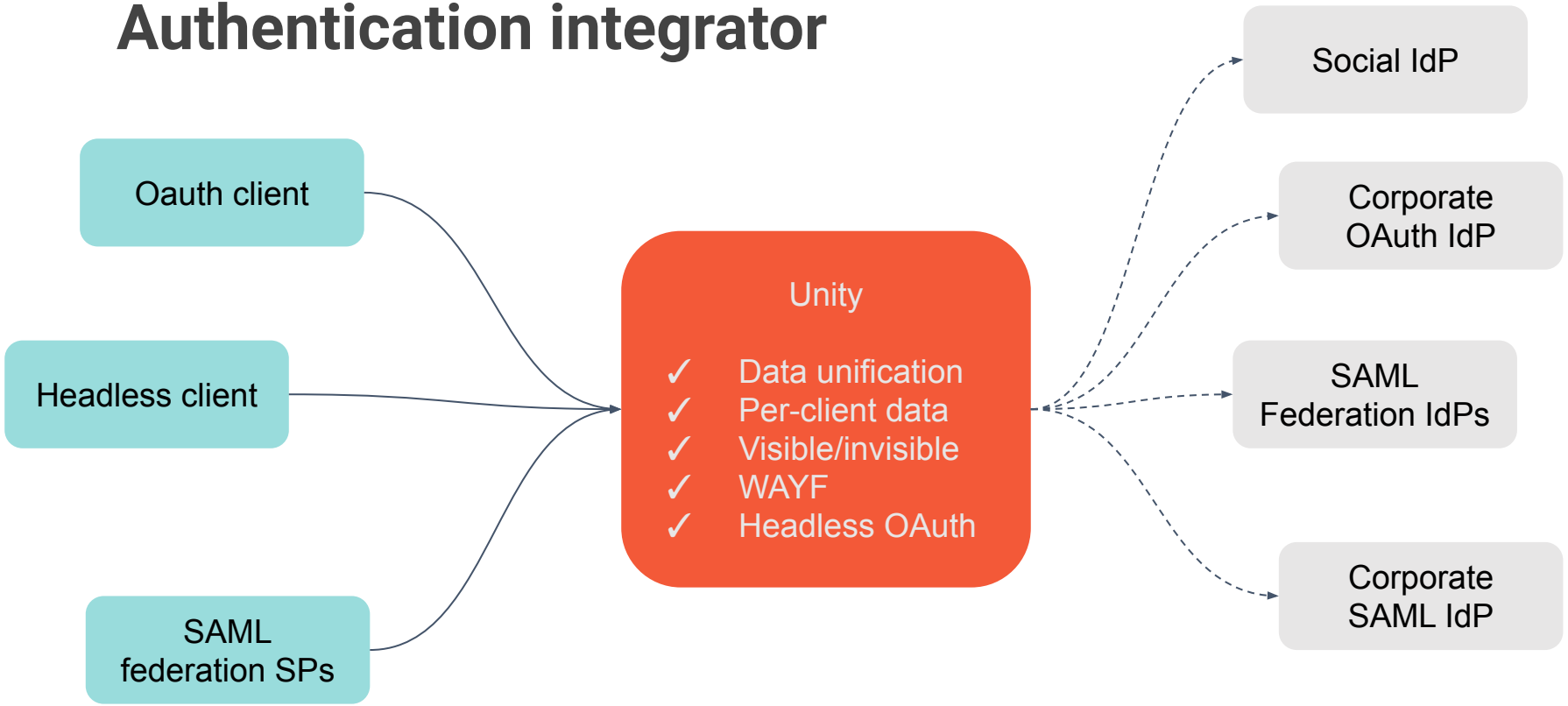
Off-the-shelf authentication service



Off-the-shelf authentication service

- Secure password handling, from storage to configurable reset
- Wide range of other supported credentials: SMS codes, OTP, Fido2, X.509
- 2FA
- Powerful and easy to use users directory
- Complete, highly configurable, users enrollment
- Simple integration with 3rd party IdPs like Google, FB, GH, MS, LiIn, …

Authentication integrator



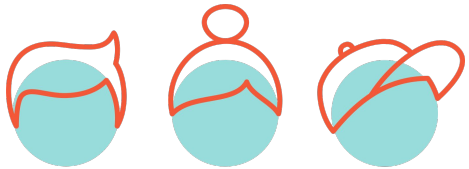
Authentication integrator

- Can delegate authentication to external IdPs
- Can be a completely invisible authentication proxy
- Or a visible proxy with native WAYF support
- Externally obtained identity material can be flexibly mapped to a unified format
- Clients may be integrated with Unity using OAuth, OIDC and SAML 2
- Uniform Unity representation of users can be presented in multiple forms per various clients and access protocols
- Possibility to plug additional, enriching attribute store (LDAP, …)

Mix & match

All of the features can be mixed in arbitrary way, the scenarios can overlap

Ecosystem

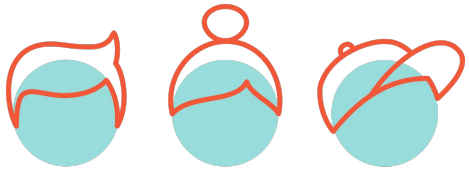


History

- Born in 2013
- The first stable release early in 2014
- Over 80 releases so far
- Long road
  - from a small private project
  - growing as an EU-funded project
  - to a sustainable product used commercially
- As of now we have/had partners and notable use cases in US, Germany, Poland, Austria and Italy
  - Both in public and commercial sectors

Open source landscape

- Unity is a truly Open Source software, BSD licensed
- We receive various open source contributions
  - Patches, complete features and translations
- We also implement feature requests coming from the community
  - Ranking them according to our perception of long term roadmap and available resources



Professional services

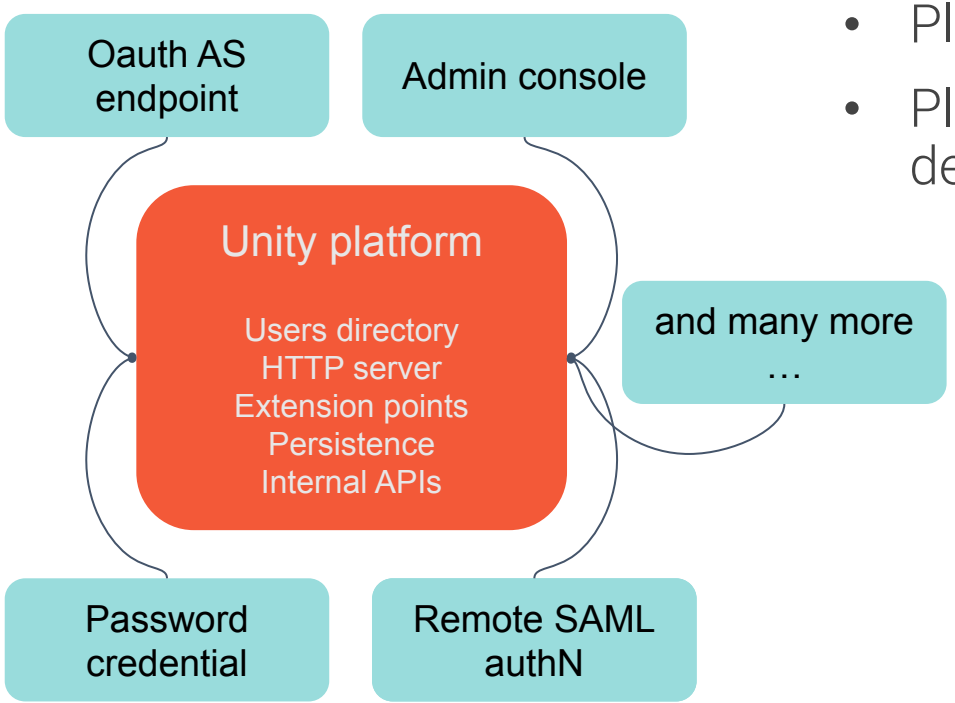
- Offered by Bixbit
  - Deployment and ops support
  - Prioritized development of requested features
  - Consulting
  - Developing software using Unity
- Launching a new trademark authvisor.com

German accents

- UNICORE was one of the early drivers for Unity development
- Unity still is in use with UNICORE deployments
- We have a great cooperation with FZJ and HZB
- Not to forget great feedback from Marcus :-)

Technical perspective

Platform + plugins



- Unity is essentially a platform with many plugin points
- Platform is not useable alone
- Plugins provide access to it and define commonly used functions
  - Endpoints,
  - Authentication methods
  - Credentials
  - Attribute types
  - Protocol bindings
  - And more…

Users directory

- Users directory is part of the Unity platform
- Entity is the main element, representing users, software agents, etc
  - Entity must have at least one Identity which is used to identify it in unique way
  - And typically has many different identities: username, email, opaque identifier, X.500 name (DN), persistent targeted identifier, and more
- Entities are organized in hierarchical groups structure
  - Member of a subgroup is always a member of parent group
- Entities may have local credentials, but that’s completely optional

Users directory: attributes

- One of the powerful features of Unity directory is attributes system
- Attribute types are defined in schema, governing value types and various constraints on values
  - Types are pluggable
  - We support strings, enums, numeric, date/time, verifiable email and many more
- Attributes can be assigned to entities in numerous ways:
  - Directly in a scope of a given group
  - Globally
  - Dynamically with a group attribute statement

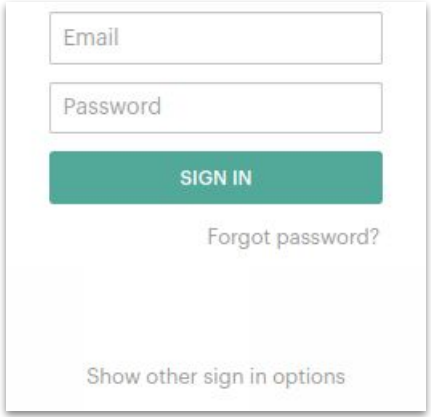
IdP endpoints

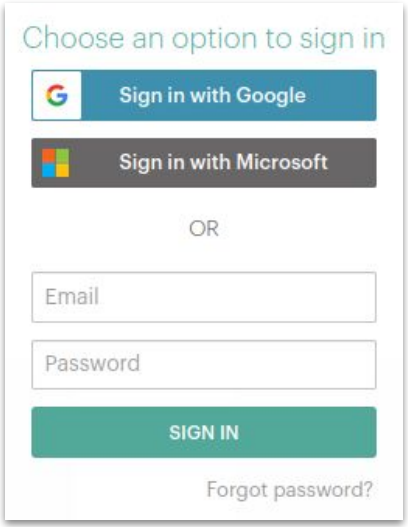
- From Unity client perspective an Identity Provider function is fundamental
- IdP functionality is implemented by several endpoints
  - Web & non-web OAuth (with support for OIDC)
  - Web SAML 2
  - SOAP SAML 2
- IdP endpoints implement their corresponding authN protocol
- Consent functionality is provided in the case of web flows

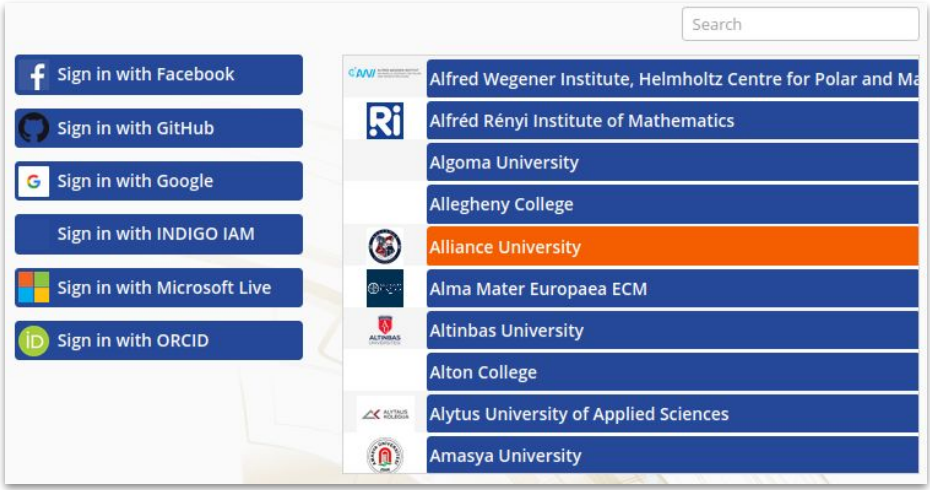
Authentication

- Authentication process is the most sophisticated part of Unity
- Three different types of authentication are supported:
  - Local: Unity collects credential and verifies it locally
  - Remote: Unity redirects to an external IdP using OAuth or SAML AuthN
  - Mixed: Unity collects credential and delegates verification to external service (LDAP, PAM)
- The above distinction is irrelevant for admins and users: all authentication facilities “feel” the same: configuration and usage wise

Authentication







Authentication: 2FA

- Besides simple, one-step authentication, Unity allows admins to define authentication flows, supporting 2FA
- Authentication flows allow for flexible configuration of 2FA rules
- SMS codes, TOTP and Fido2 are the credentials typically used as a 2nd factor
    - But authentication flow can be configured in arbitrary way
- Unity natively handles all credentials, with big help of libraries

Remote authentication

- Remote authentication (regardless of how credential is collected) requires mapping of external entity to an internal one
- The process is unified for all types of external authentications and handled with remote data processing profiles
    - The same approach regardless if a user is coming from LDAP, Shibboleth or Google
- Processing profile is translating the obtained attributes to a unified (admin controlled) form
    - mapping of external entity to Unity one is the key step
    - number of additional actions can be enabled, as entity blocking

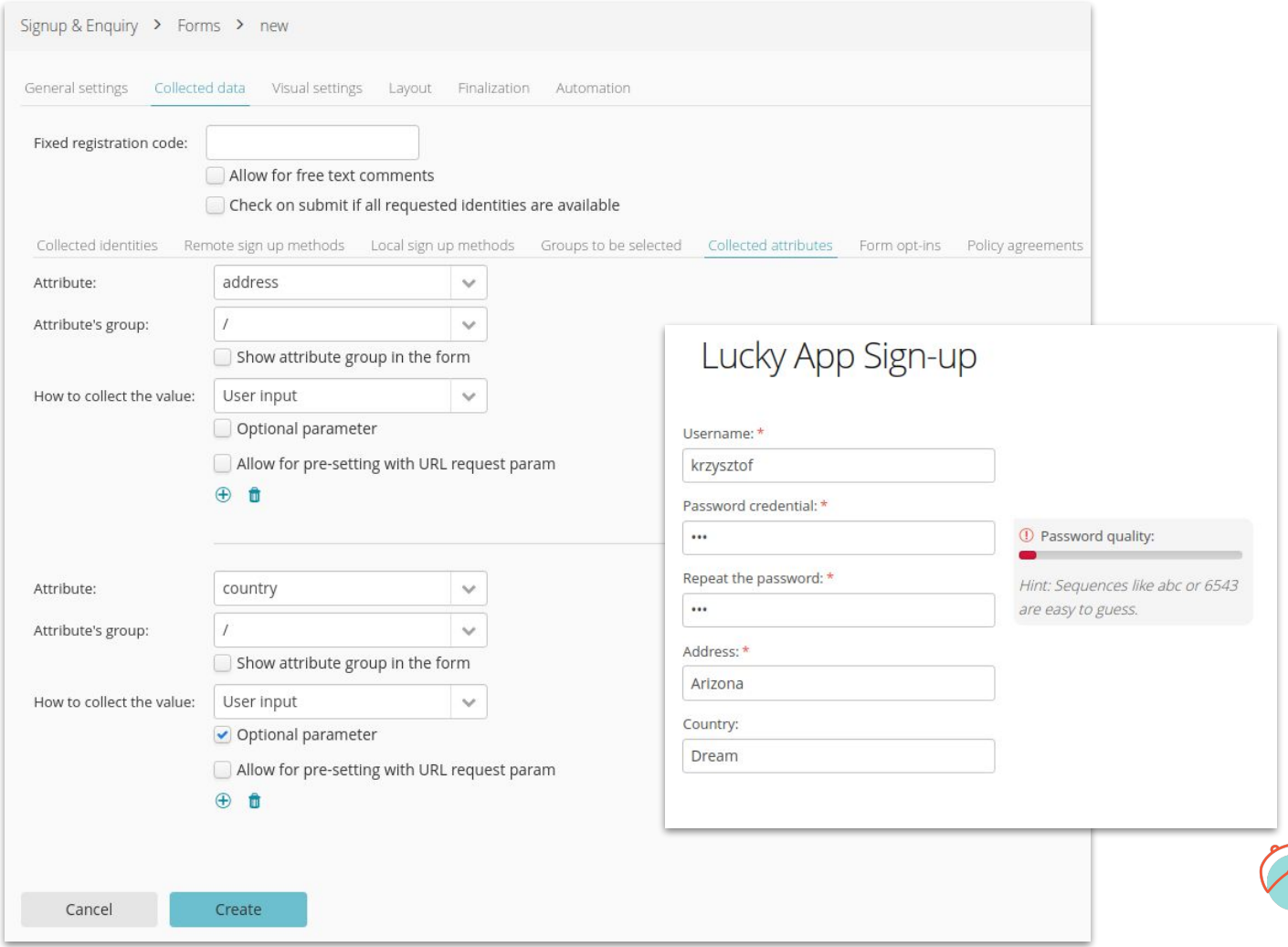
Sign-up

- Even a great sign-in has a little value w/o sign-up
- User can be registered:
  - with a help of standalone form, under a public URL
  - by filling a form launched from a sign-in page
  - as a result of remote authentication when remote user is not mapped to an existing Unity user
  - by invitation
- Sign-up can be fully local, or may use external IdP
  - The latter case is a powerful & often used feature

Sign-up forms

- Administrator can configure many registration forms
- Forms decide what data should be collected and in what way
  - Attributes, identities, credentials, policy agreements
- Advanced aspects like confirmation of emails or mobile numbers are supported
- The submitted registration request can be processed automatically with a help of special translation profile
  - Resembling remote data processing during authentication
  - New attributes can be created, data cleaned, etc
- Requests can be accepted manually or automatically with dynamic conditions
- Wide range of notifications is supported

Sign-up forms



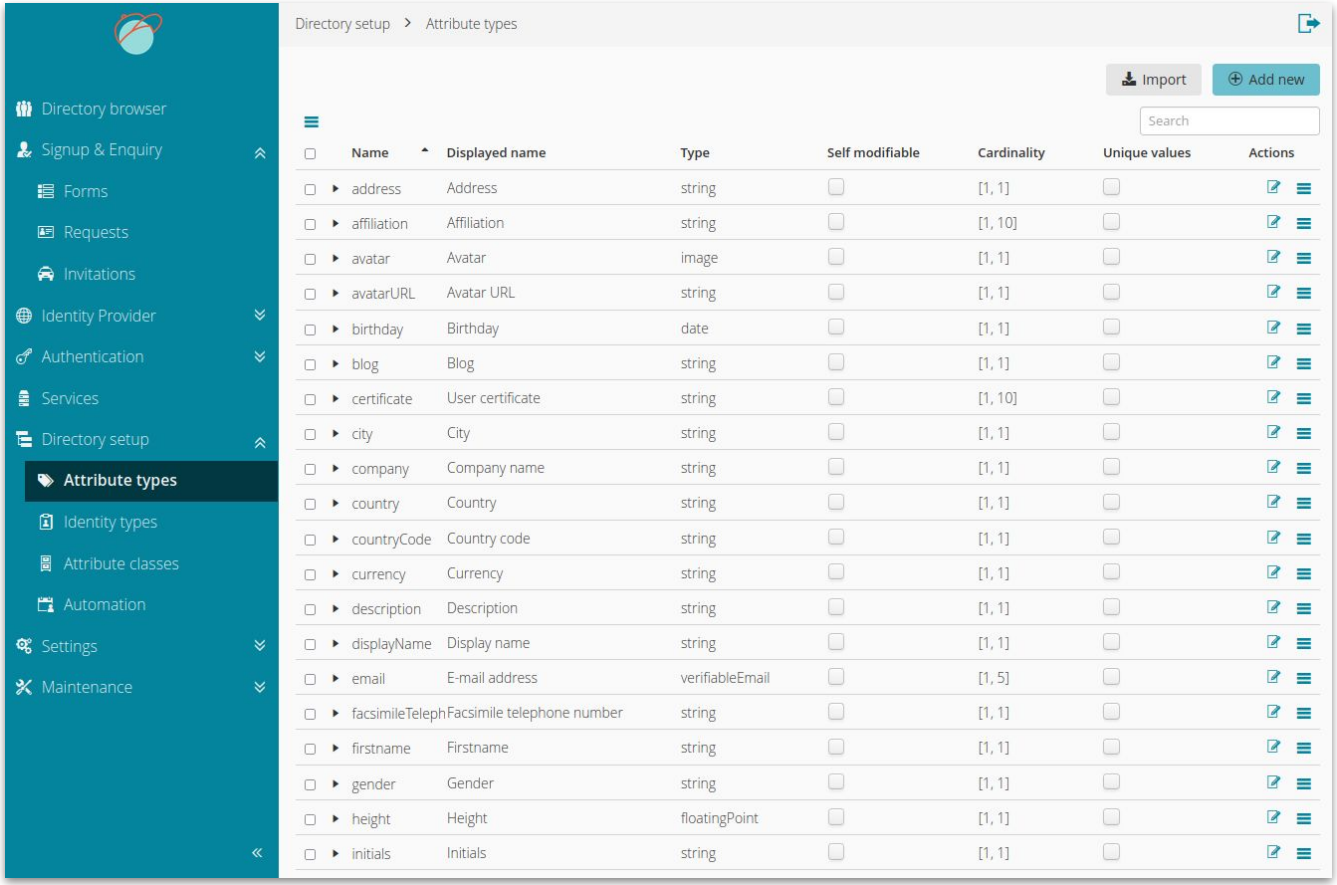
End-user oriented endpoints

- User’s account endpoint provides a “profile & settings” features
  - Useful if integrated application(s) do not offer their own profile screen
- Unity Project Management (UpMan) is an endpoint targeted at users who should have a limited Unity group administrator capabilities
  - Groups represent VOs, community, projects, etc
  - Allows for managing group users, invite new, remote etc.

Administrative endpoints

- Administrative interfaces are regular endpoints
  - Configurable authentication and everything else like in any other endpoint case
- Web UI is offered by the Console endpoint
- A proprietary REST API endpoint allows for software integrations
- Since recently we also offer a RO SCIM REST endpoint with a fully configurable schema

Console


Directory setup
Attribute types
Import
Add new
Search
Directory browser
Signup & Enquiry
Forms
Requests
Invitations
Identity Provider
Authentication
Services
Directory setup
Attribute types
Identity types
Attribute classes
Automation
Settings
Maintenance
Name
Displayed name
Type
Self modifiable
Cardinality
Unique values
Actions
address Address string [1, 1]
affiliation Affiliation string [1, 10]
avatar Avatar image [1, 1]
avatarURL Avatar URL string [1, 1]
birthday Birthday date [1, 1]
blog Blog string [1, 1]
certificate User certificate string [1, 10]
city City string [1, 1]
company Company name string [1, 1]
country Country string [1, 1]
countryCode Country code string [1, 1]
currency Currency string [1, 1]
description Description string [1, 1]
displayName Display name string [1, 1]
email E-mail address verifiableEmail [1, 5]
facsimileTeleph Facsimile telephone number string [1, 1]
firstname Firstname string [1, 1]
gender Gender string [1, 1]
height Height floatingPoint [1, 1]
initials Initials string [1, 1]

Other notable features

- Advanced notification subsystem
  - Message templates
  - Email, SMS and custom (groovy script) channels
  - Unity can be your message sending gateway
- Policy documents framework
  - Defining policy documents
  - Binding acceptance to various points
- Audit log

Other notable features (2)

- Branding
- Extending with scripts
  - Groovy
  - Post-startup initialization & hooks to hundreds of operations
- Native, selective, JSON backup and restore
- Automation rules
- Separation of SSO areas with Authentication Realms
- Attribute introspection endpoint helping to integrate remote IdPs
- Account linking
- User enquiries

Tech stack

- Java 11 + Spring core
- Modularized monolith
  - 36 maven modules currently
- RDBC based storage
  - MySQL, MariaDB
  - PostgreSQL
  - H2 (testing/demo only)
  - non-RDBC based storage is possible, for some time we had Hazelcast storage backend
- UI is based on Vaadin 8

Future plans

- Update to Vaadin 23+
  - modern web toolset, web components based
  - In progress
- Revamp of the User’s Account Service (HomeUI)
  - In progress (early)
- Java 17
- Performance improvements for large deployments
- Features, features, features, …

Companion solutions

FURMS

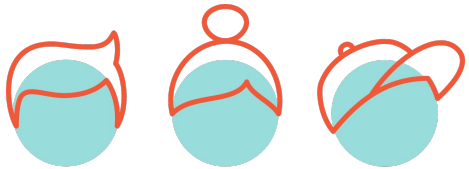
- Tool developed for the Fenix consortium; https://fenix-ri.eu
- Fenix User & Resource Management Service
- Open Source; https://unity-idm.github.io/furms
- Mature, polished and commercially supported software allowing for:
  - Provisioning of resources by providers (sites, like HPC centers)
  - Distribution of available resources using 2-level model (central and community) to projects
  - Recording, visualising and monitoring of resource usage, with help of site agents

Devops tooling

- A new kid in our family
- https://github.com/unity-idm/unity-devops
- A set of Ansible scripts allowing sysadmins to:
  - Install and update deployments
  - Start and stop instance
  - Automatically structures deployment using a proven filesystem layout
  - Backup and restore

And more…

- Some of the developed applications are proprietary & confidential
- We are in early stage of discussing a new tool to handle VO management



Resources

Webpage:
https://unity-idm.eu

Commercial support:
https://www.authvisor.com

GitHub:
https://github.com/unity-idm/unity