UNIfied identiTY management

Krzysztof Benedyczak
ICM, University of Warsaw

The idea

Identity and Authentication Management as a Service

- Multiple authentication protocols supported
  - easy integration with various consumers/clients.
- Ability to outsource credentials (and attributes) management to a 3rd party service.
  - Multiple upstream protocols supported.
  - UNITY becomes a bridge (protocol translation)...
  - ... and a hub (single service aggregating various IdM systems).
- Embedded, users directory with advanced management.

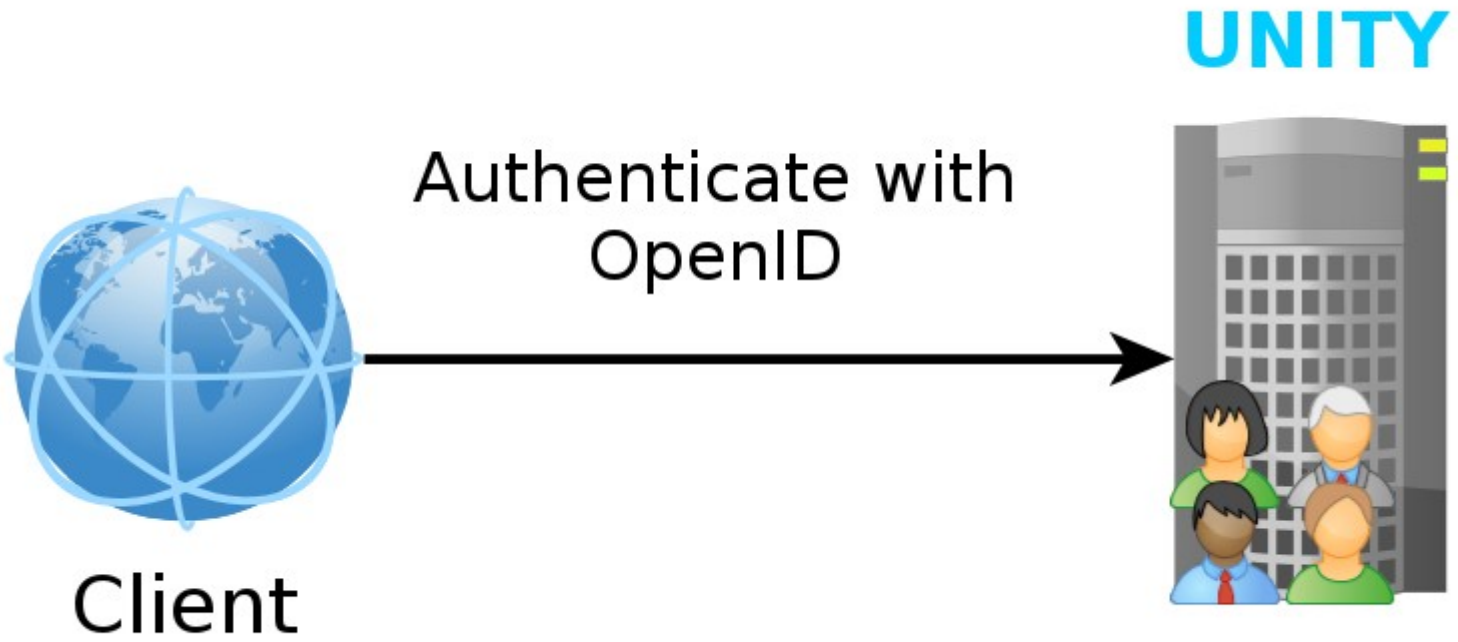
Highlights

- Highly useful for cloud applications.
  - Web-based management, many web protocols supported.
- Built as an extensible container tuned for IAM
  - Credentials, endpoints, external authentication methods, credential retrieval methods and many others are pluggable.
- Contains an embedded, full-blown users, groups and attributes database.
- Frequent updates (around 10/year).

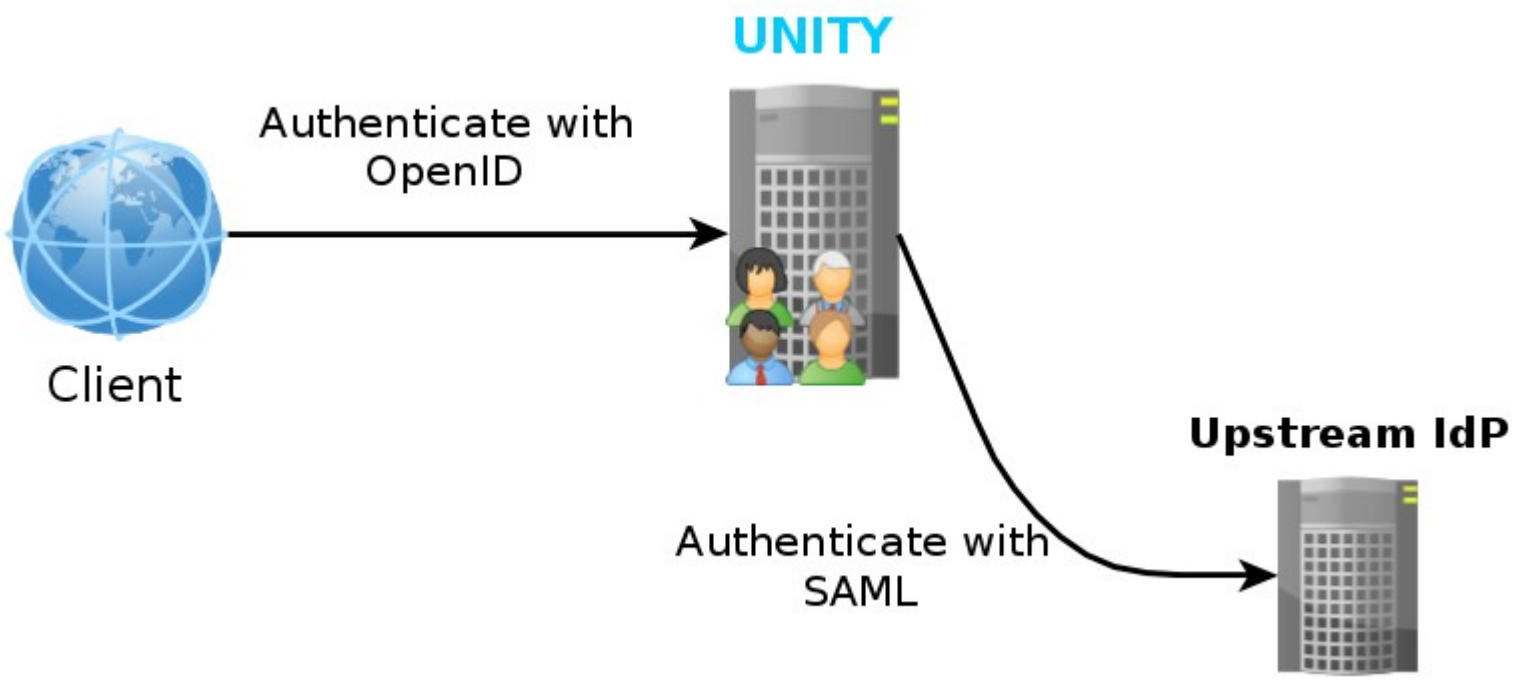
Local database

- Unity features a full-blown, embedded users directory
  - Multiple identities per user, may have various types
  - Attributes, attribute classes, scoped visibility
  - Credentials, credential requirements
  - Hierarchical groups
  - Advanced features as attribute statements (=> automatic attributes).

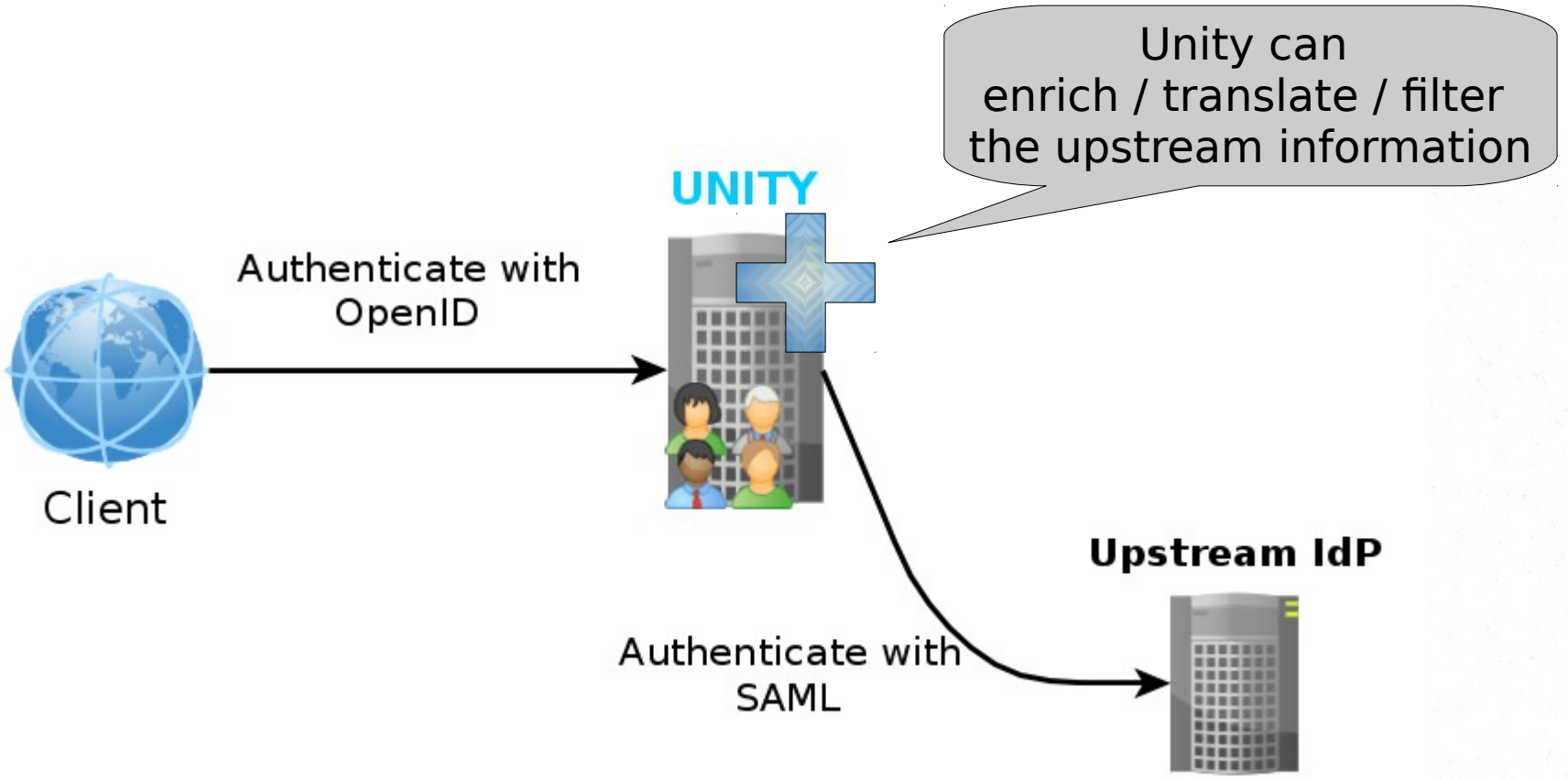
Authenticate



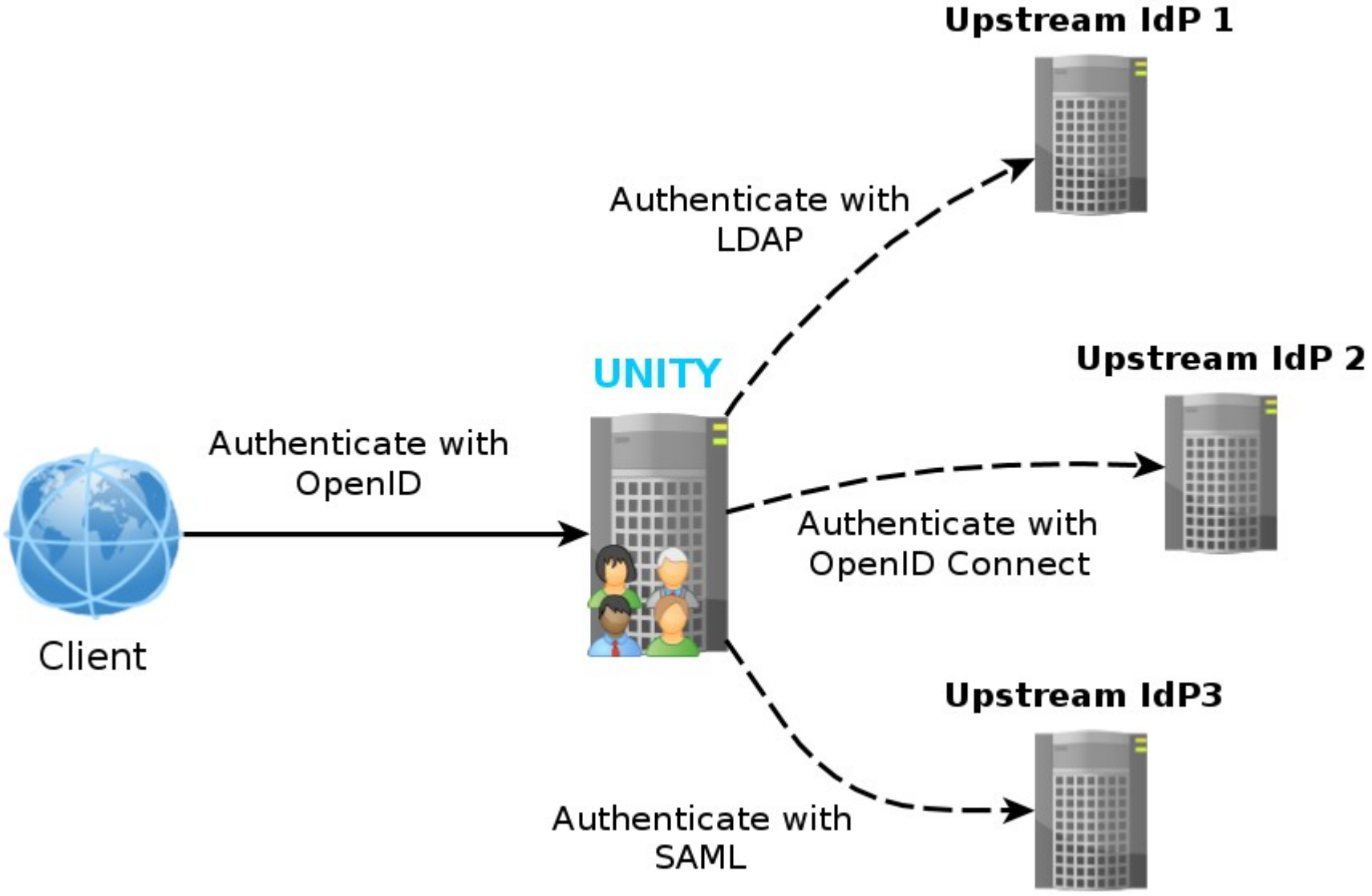
Remotely authenticate, translate protocol



Process remote user data



Orchestrate



Overall status

- Unity is still very young
  - Unity *idea* was born at the beginning of '13
  - Development started late February '13
  - The first stable release mid January '14
  - The first update last Monday
- This doesn't mean that it bears the common symptoms of immature software
  - 6 Milestone and RC releases
  - Extensive documentation
  - Strict development process: high test coverage, regular static code analysis, code reviews, ...

Stakeholders & sustainability

- PL-Grid Plus & PlusPlus projects are going to use Unity for UNICORE infrastructure.
  - Deployment tests started
  - Will need to be maintained for ca 7 years from now.
- Several other projects interested as LSDMA.
- Unity is not strictly PL-Grid bound. It is a more general ambition to create a universal IAM solution which is missing piece in many cases.
- Unity has a commercial potential.

Features status

- Container mostly complete
  - Though several important features missing as HA deployment tooling.
- Local users database mostly complete
  - However only two credentials implemented: password and X.509 certificate.
- SAML endpoints (Web and SOAP) available
- External LDAP and SAML authentication.
- Base support for registrations available.
- Large part of Web Admin UI is ready.

The future (highlights)

- Improved SAML support
- Redundancy/HA tests and tooling
- OpenID endpoint
- OAuth 2 AS endpoint
- External OpenID authN
- Support for other external authN protocols (as OAuth authN, OpenID Connect, Kerberos)
- New credentials (e.g. one time passwords)
- Auditing
- User driven groups
- ***Respond to community requests***
- *and many others... e.g. RBA*