Access Management 2.0: UMA for the Enterprise

@UMAWG

3 June 2014

tinyurl.com/umawg

Agenda

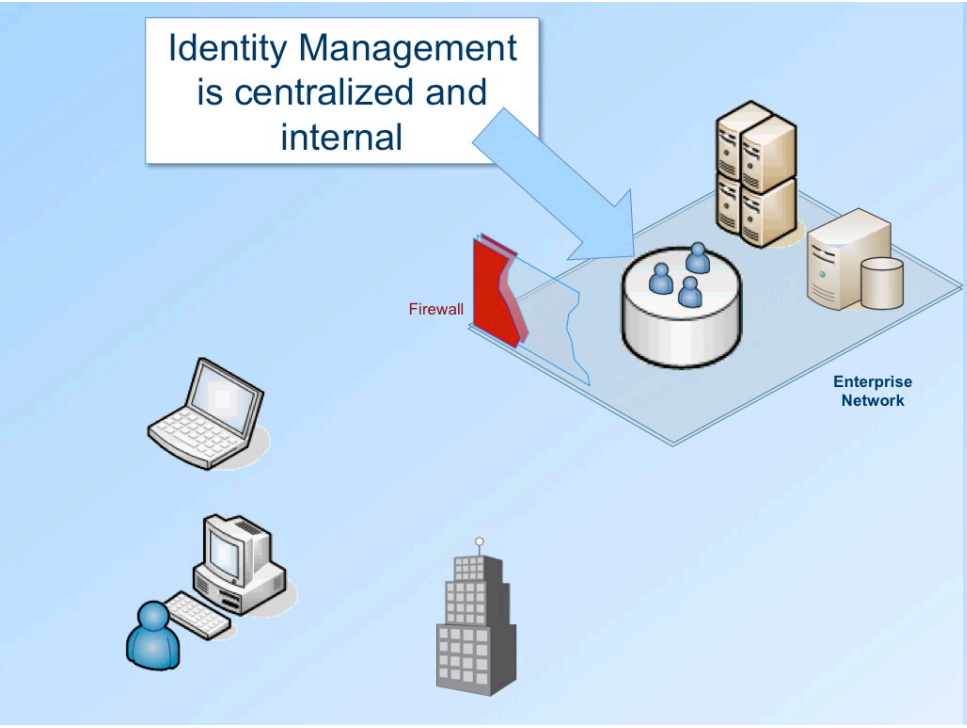
- The realities and challenges of modern access control
- “UMA for the Enterprise 101”
- What vendors are saying and doing about UMA
- Q&A

Further reading:
tinyurl.com/umaam20

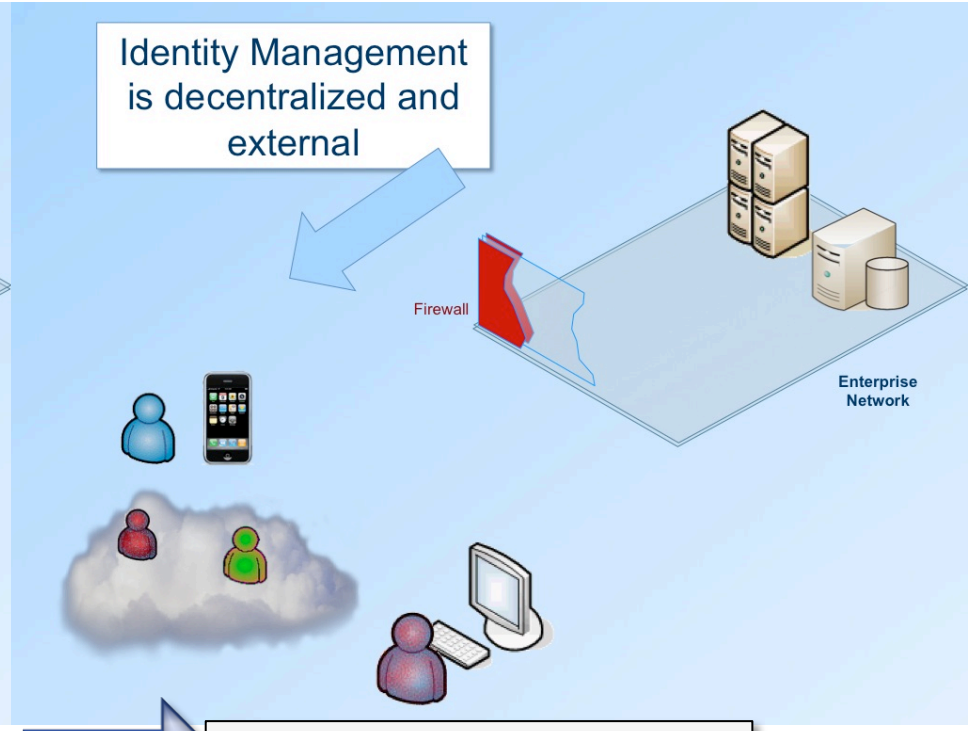
The realities and challenges of modern access control

UMA Continues The Shift In Identity Management That Began With OAuth

The Traditional Enterprise



The 21st Century Enterprise



This is the secret to achieving scale and agile federation

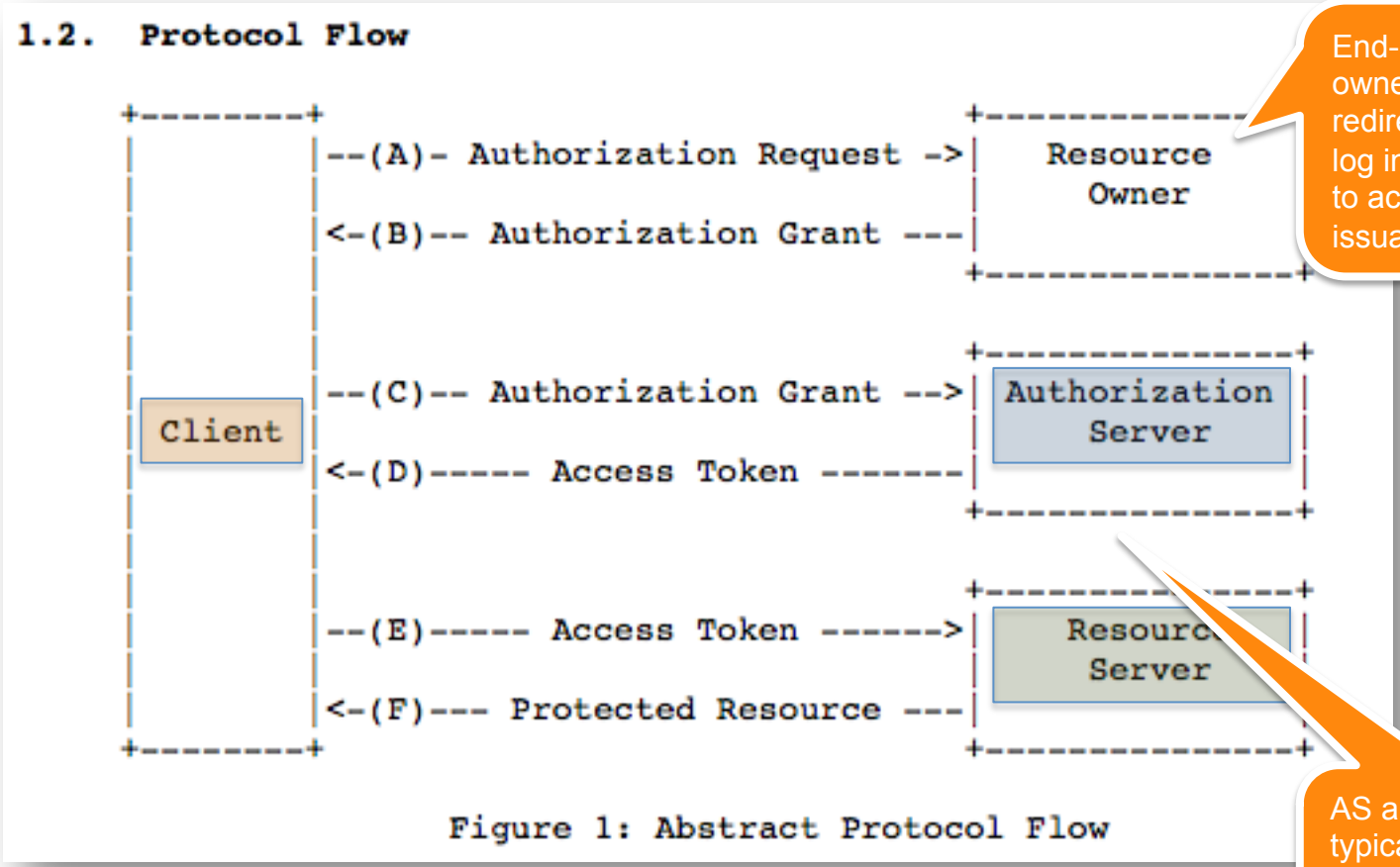
Key issues expressed

- Noncentralized nature of OAuth trust model
- Variety of nondiscretionary policy sources
- Need inexpensive, dev-friendly, mobile-ready, API-capable entitlements
- “Headless” resource owners
- Need third parties to respect enterprise’s “authorization as a service”
- …Need comprehensive IoT security model

Further reading:
tinyurl.com/umafaq

“UMA for the Enterprise 101”

OAuth is a three-entity protocol for securing API calls in a user context

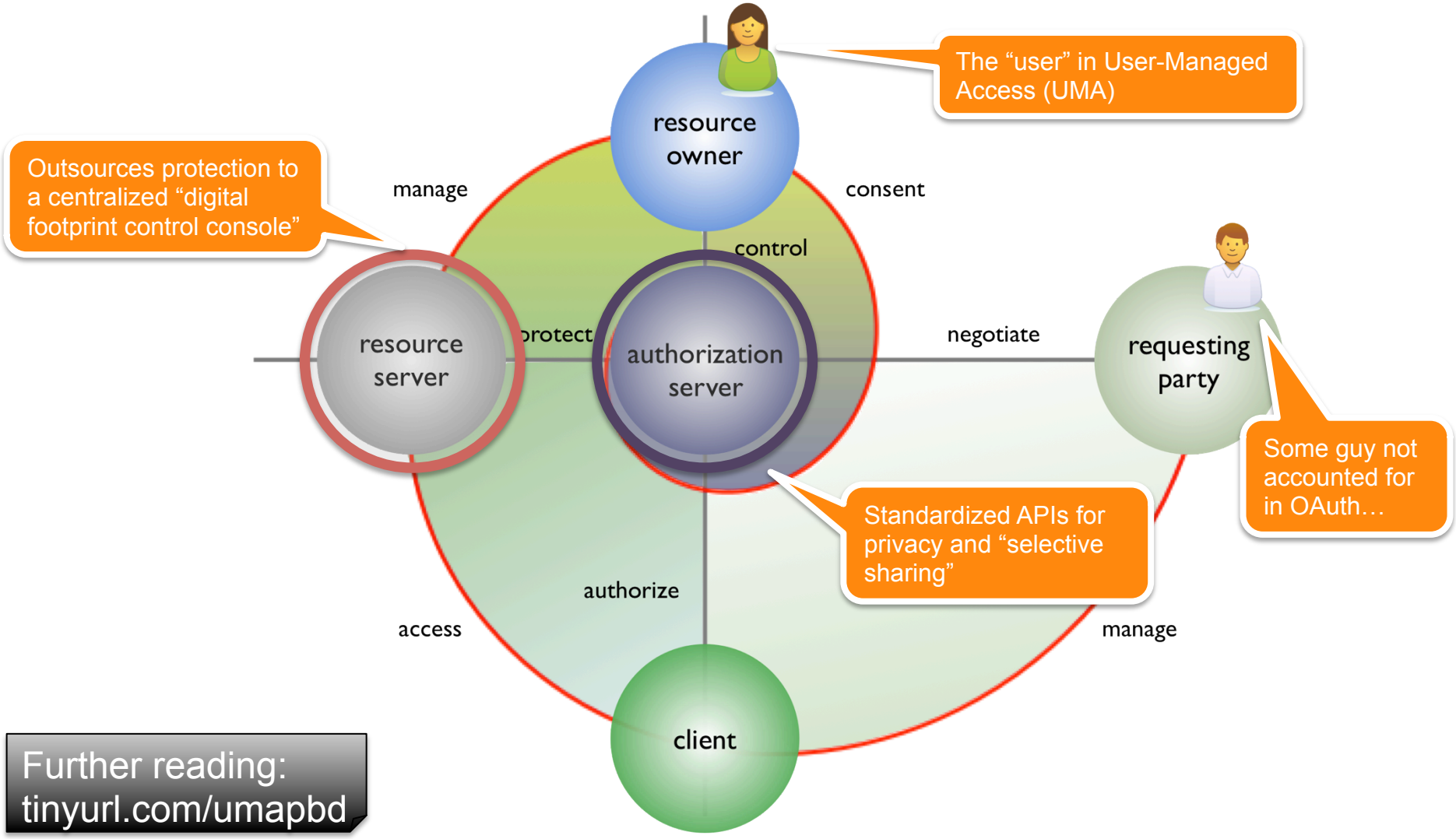


End-user resource owner gets redirected to AS to log in and consent to access token issuance

AS and RS are typically in the same domain and communicate in a proprietary way

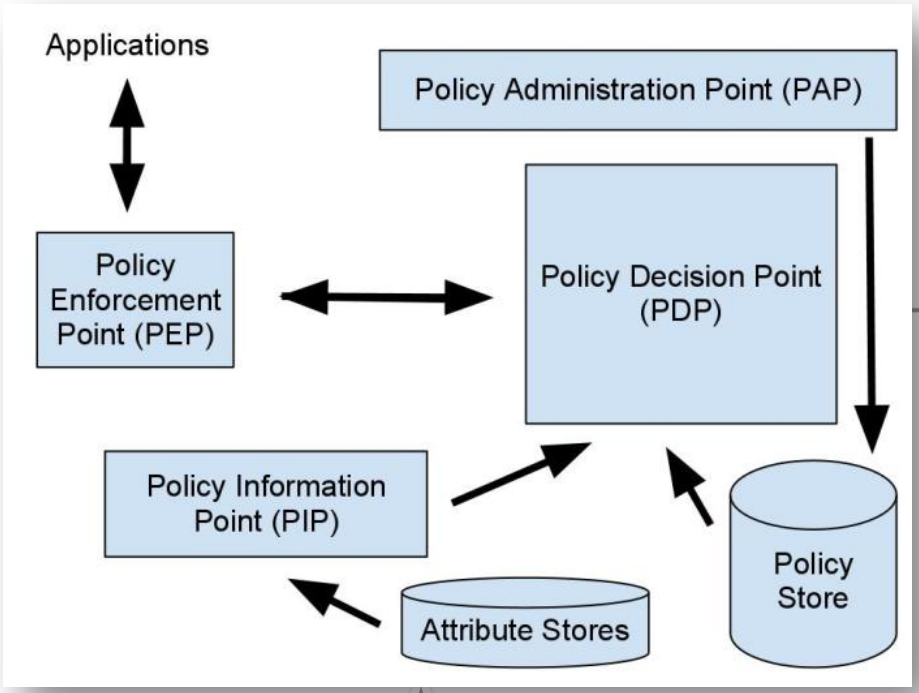
Source: The OAuth 2.0 Authorization Framework, http://tools.ietf.org/html/rfc6749

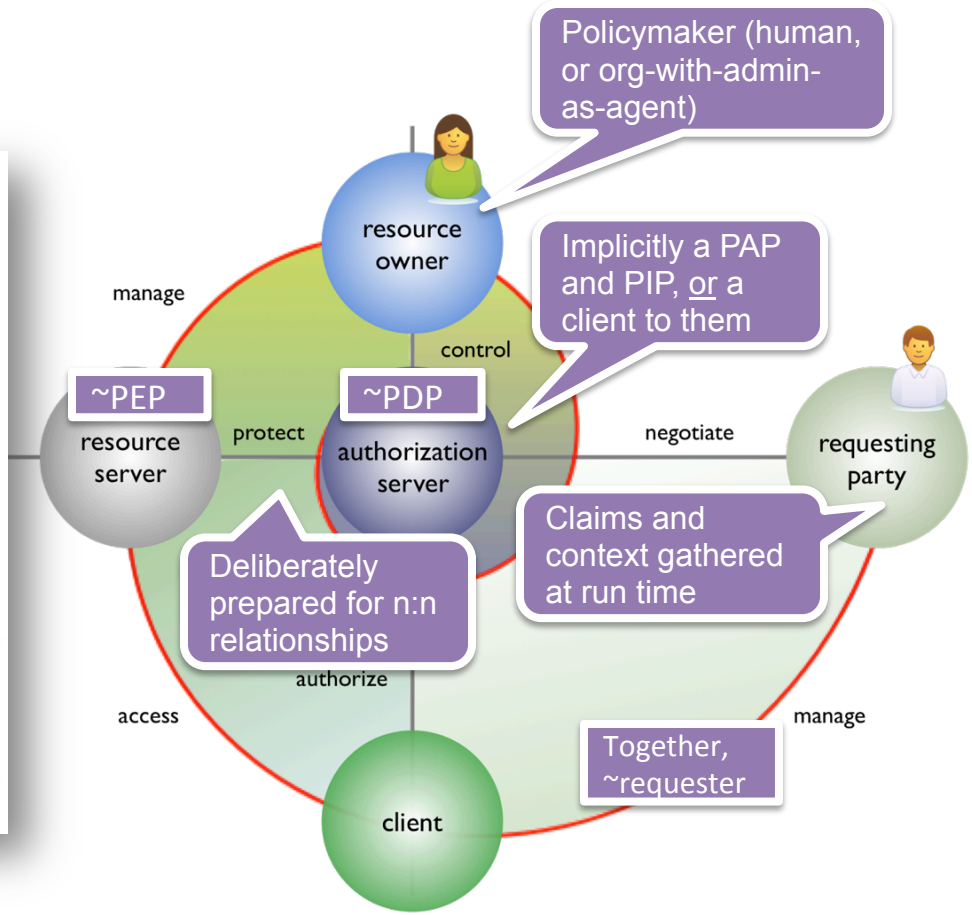
UMA's original goal: apply privacy-by-design to OAuth data sharing



Further reading:
tinyurl.com/umapbd

Emergent UMA properties: flexible, modern, claims-based authorization

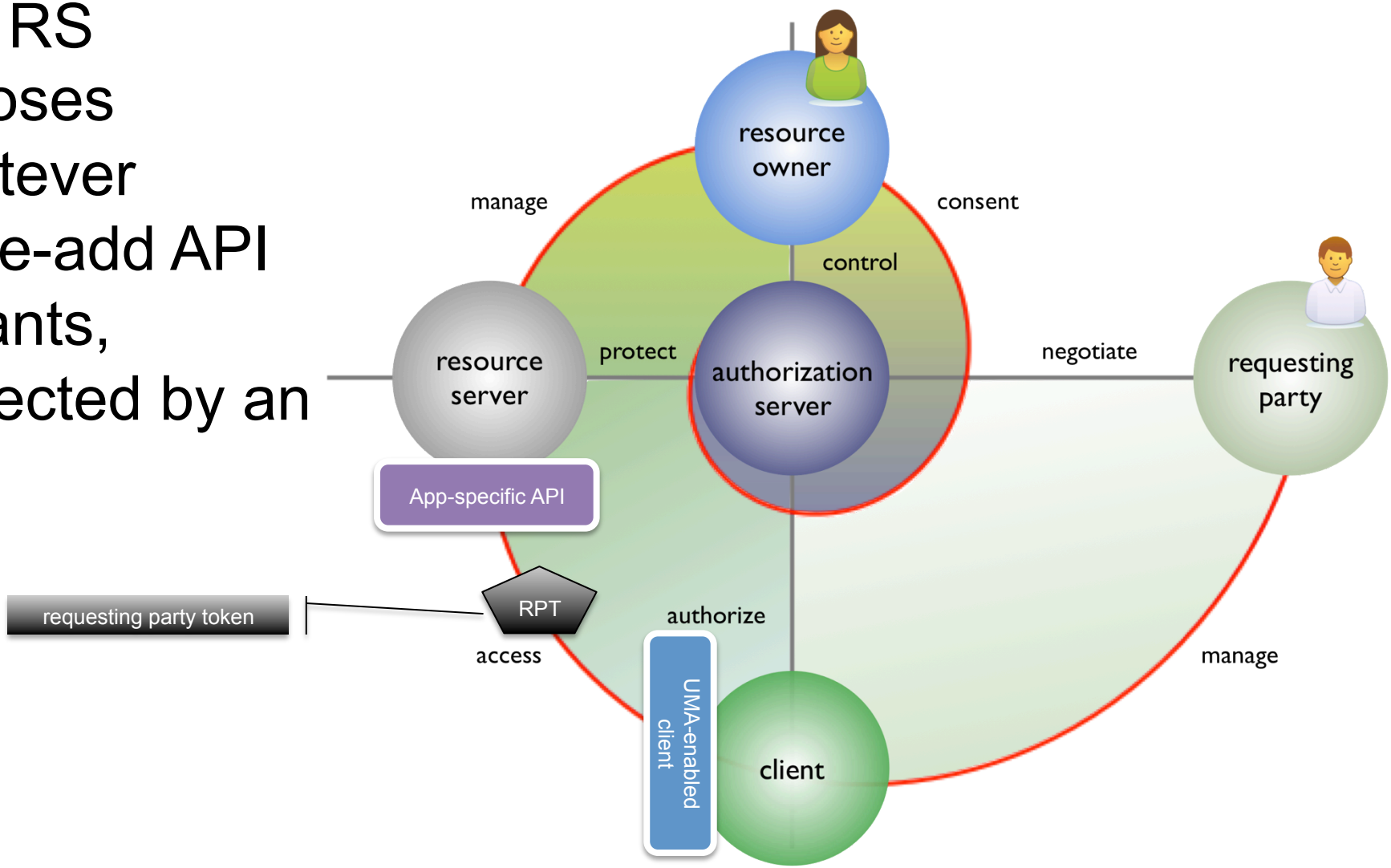




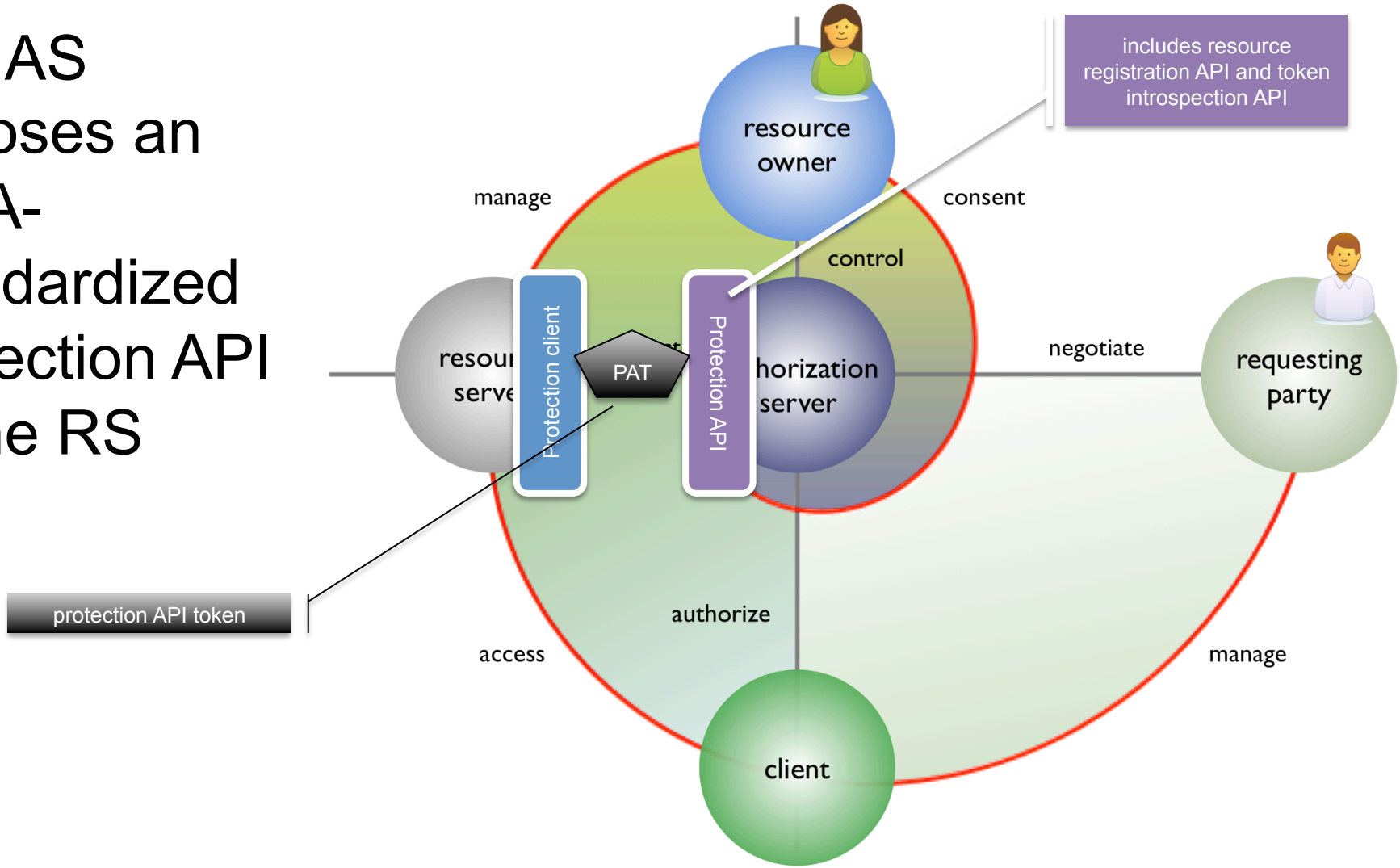
UMA and XACML can coexist nicely

Source: XACMLinfo.org, http://xacmlinfo.org/2011/10/30/xacml-reference-architecture/

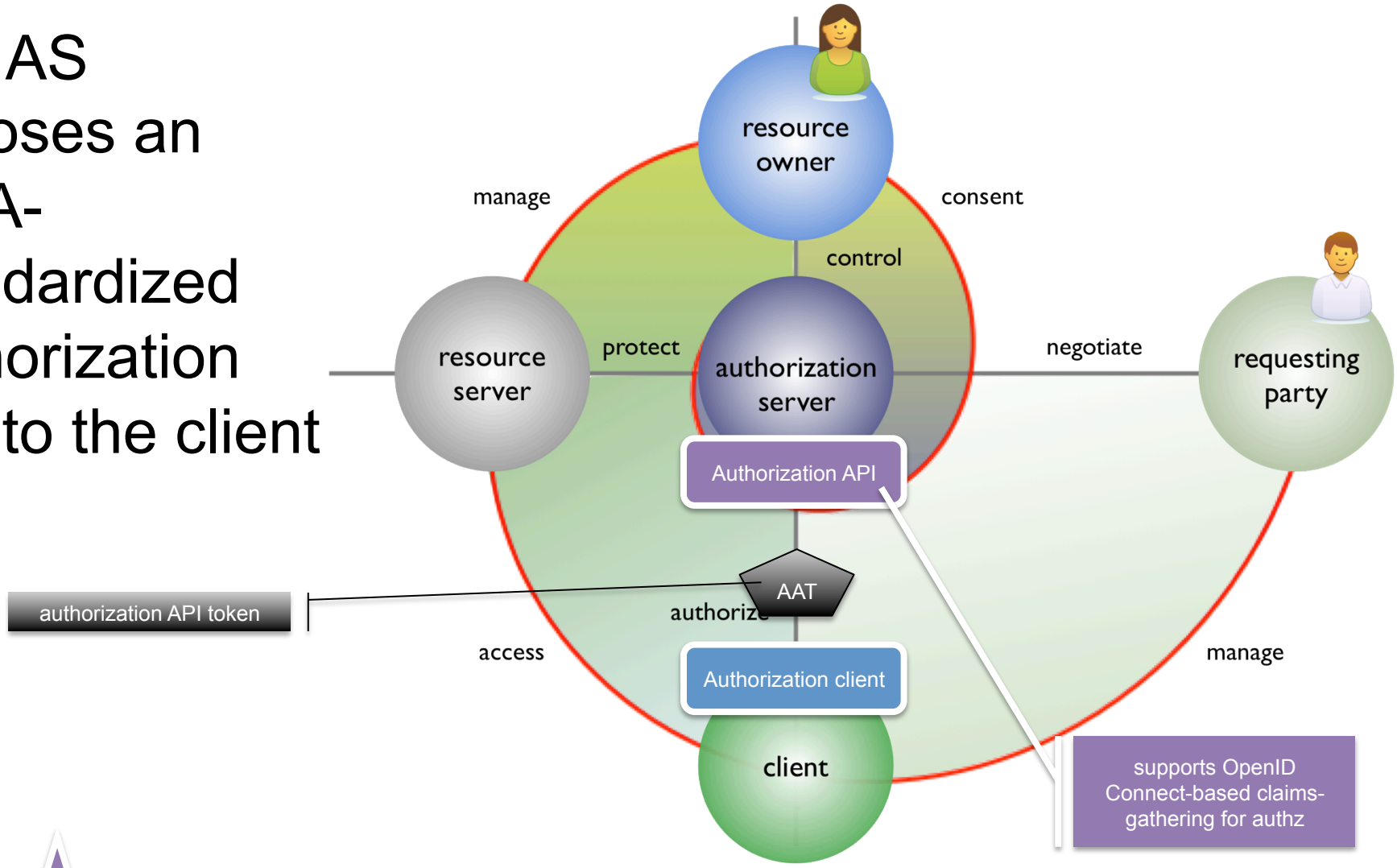
The RS exposes whatever value-add API it wants, protected by an AS



The AS exposes an UMA-standardized protection API to the RS



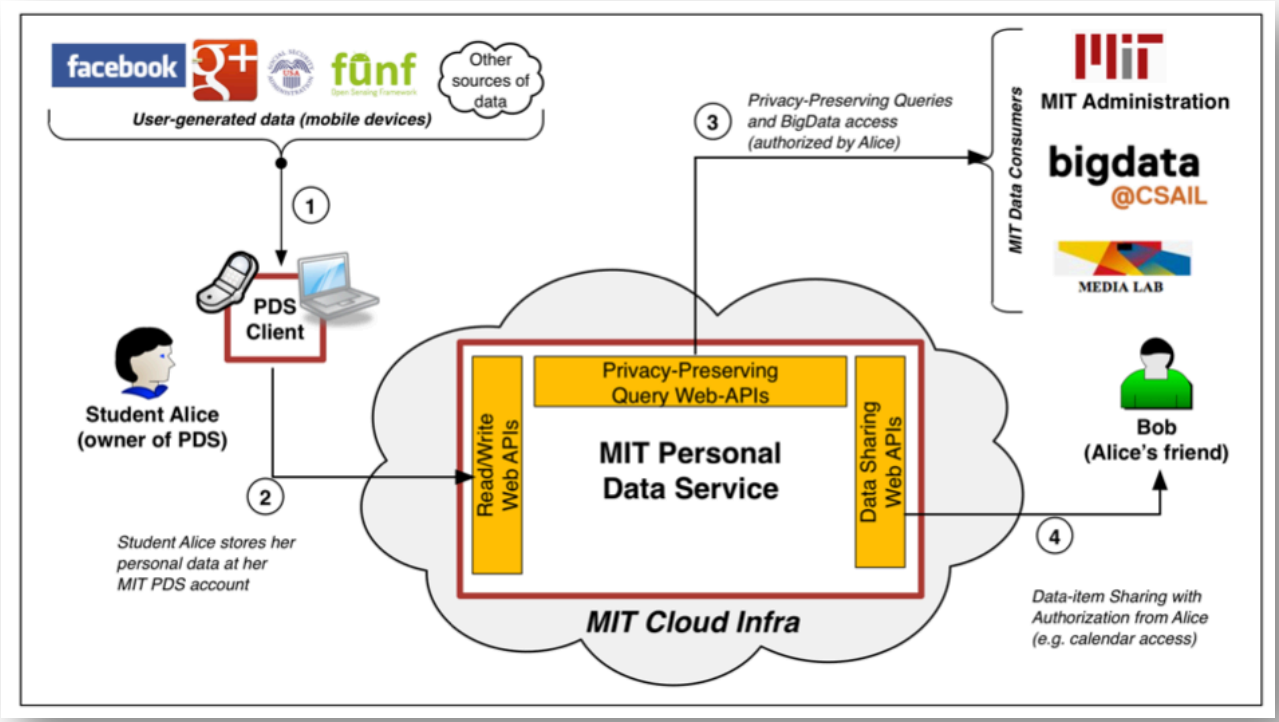
The AS exposes an UMA-standardized authorization API to the client



UMA, SAML, and OpenID Connect can coexist nicely

Key use cases

- Managing personal data store access
- E-transcript sharing
- Patient-centric health data access
- …and enterprise access management 2.0



Source: MIT Consortium for Kerberos and Internet Trust, https://kit.mit.edu

AM1.0 vs AM2.0

- Complex and feature-rich
- Usually proprietary
- Mobile/API-unfriendly
- Brittle deployment architecture
- Not agnostic to authn method
- Hard to source distributed policies
- Usually coarse-grained

- RESTful and simpler
- Standard interop baseline
- Mobile/API-friendly
- Just call authz endpoints vs. deploying an agent
- Agnostic to authn method and federation usage
- Flexible in policy expression and sourcing
- Leverages API's "scope-grained authorization"

Further reading:
tinyurl.com/uma1iop

What vendors are saying and doing about UMA

Gluu support

- Full UMA implementation in OXauth, Gluu's open-source code base
- Gluu server offers UMA protection over its SCIM API support
- Developed crowdfunded (with ForgeRock and others) open-source Apache plugin supporting OpenID Connect and UMA
- Working with ForgeRock, WSO2, and others on Canonical's Ubuntu Juju appsec framework using "new Venn of access control" elements

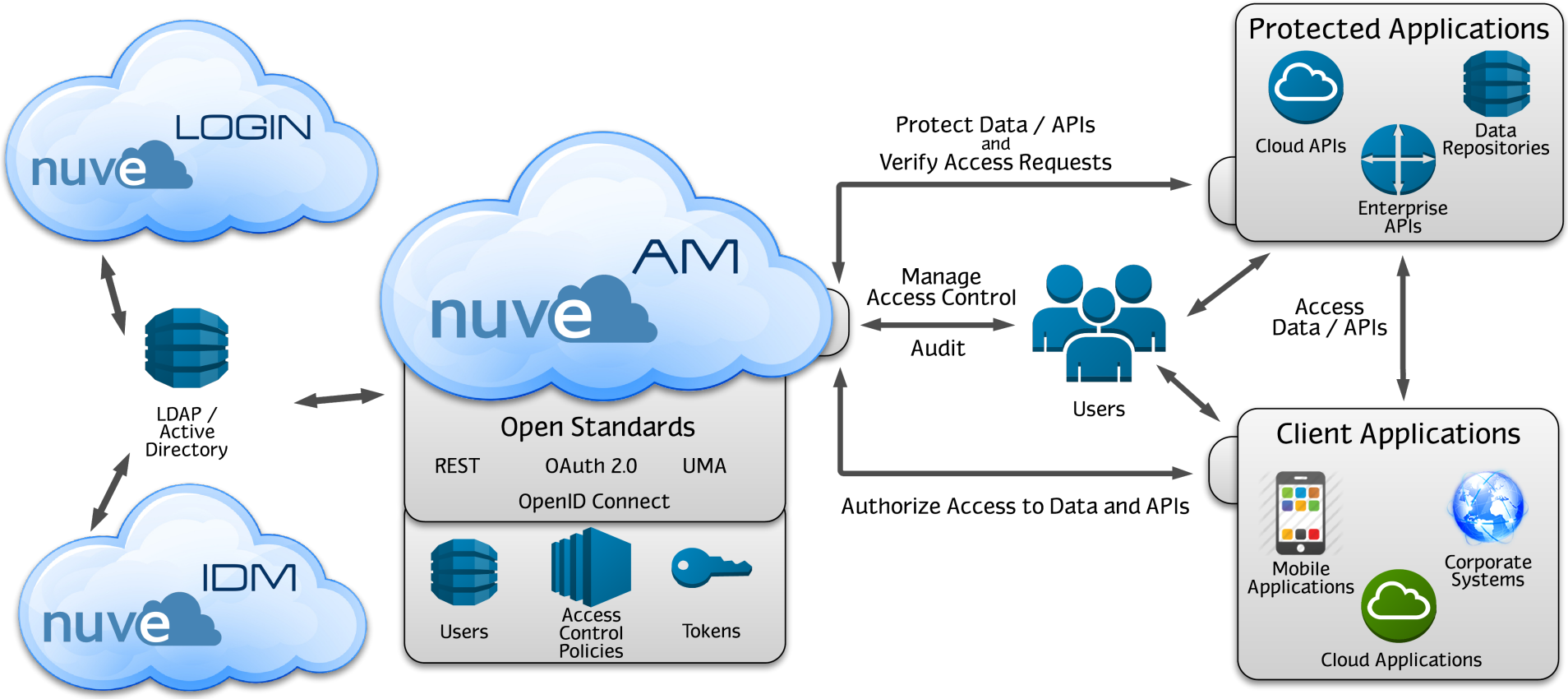
NuveAM by Cloud Identity

- UMA-compliant AS:
  - Access control to Web data
  - API security and management
  - Real-time monitoring and audit

- Use cases: Securing Personal Data Services (PDS) and access management 2.0 (API security)
- Uses open standards, including UMA, OAuth 2.0, OpenID Connect, and SAML 2.0
- Open source frameworks: Java and Python
- Support for mobile (Android)
- Integrates with Identity Management and Identity Federation

http://www.cloudidentity.co.uk/products/nuveam

NuveAM by Cloud Identity

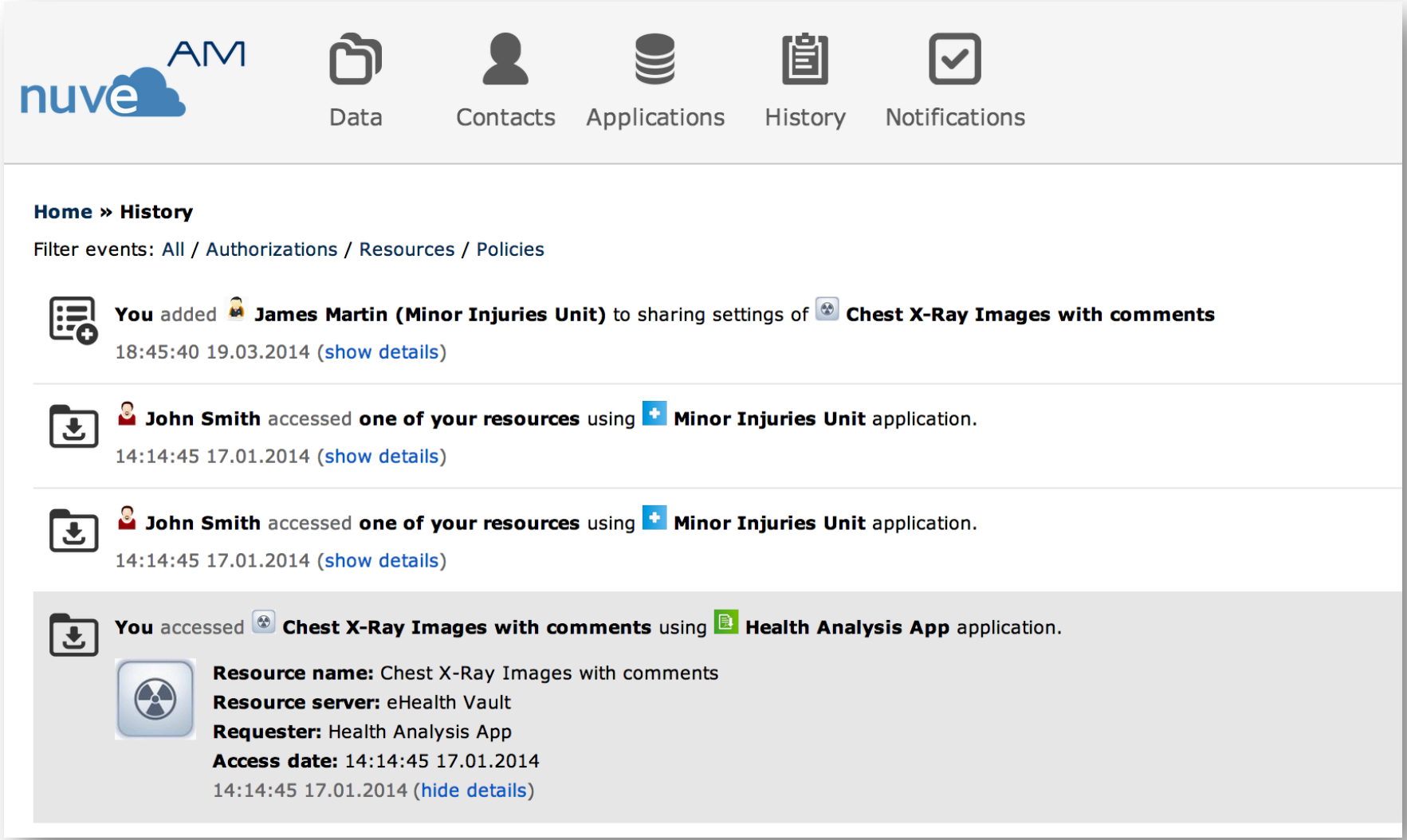


cloudidentity

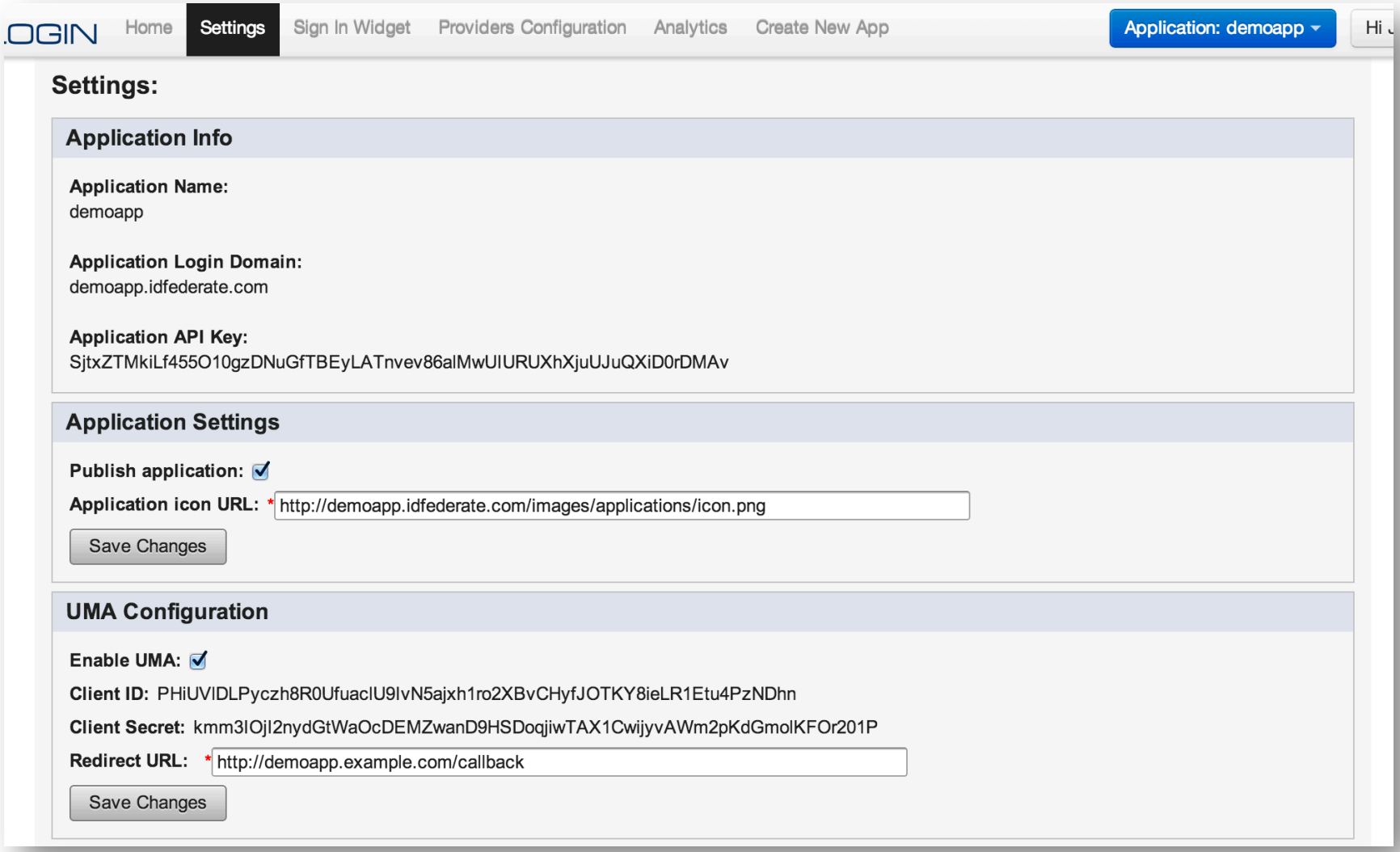
NuveAM for the enterprise

- Management of resources, APIs, permissions, and access control policies
- Access control on demand
- Detailed audit information
- Application management: resource servers and clients (with NuveLogin)
- Integration with identity management
- Integration with identity federation and SSO

NuveAM for the enterprise



NuveAM for the enterprise



ForgeRock

- Experimental UMA implementation under way

Next steps

Next steps for the WG…and you

- Get involved!
  - Become an “UMAnitarian” (it’s free)
  - Participate in the interop and our implementation discussions
  - Follow and engage with @UMAWG on Twitter
- Current work:
  - Technical: claim profiling to allow claim-gathering using SAML, OpenID Connect, LDAP…
  - Business: Binding Obligations spec to tie “terms of authorization” to multi-party state changes
- Sign up for our next webinar on June 19: UMA and Personal Clouds

Join at:
tinyurl.com/umawg

Questions? Thank you!

@UMAWG

3 June 2014

tinyurl.com/umawg