

Access Management 2.0: UMA for the Enterprise

@UMAWG

#UMAam20 *for questions*

20 March 2014

tinyurl.com/umawg *for slides, recording, and more*



Agenda

- The realities and challenges of modern access control (CA)
- “UMA for the Enterprise 101”
- Enterprise UMA case study and demo (Gluu)
- What vendors are saying and doing about UMA
- Q&A



Thanks to CA Technologies for sponsoring this webinar!



Thanks to Kantara for supporting the UMA work!

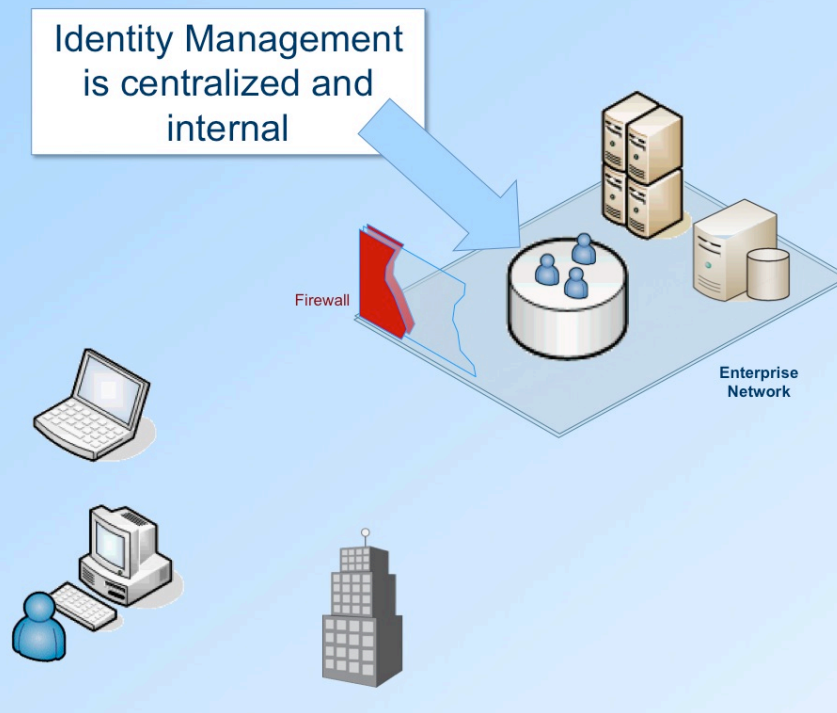


Thanks to our additional webinar participants!

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

Further reading:
tinyurl.com/umafaq

“UMA for the Enterprise 101”

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

1.2. Protocol Flow

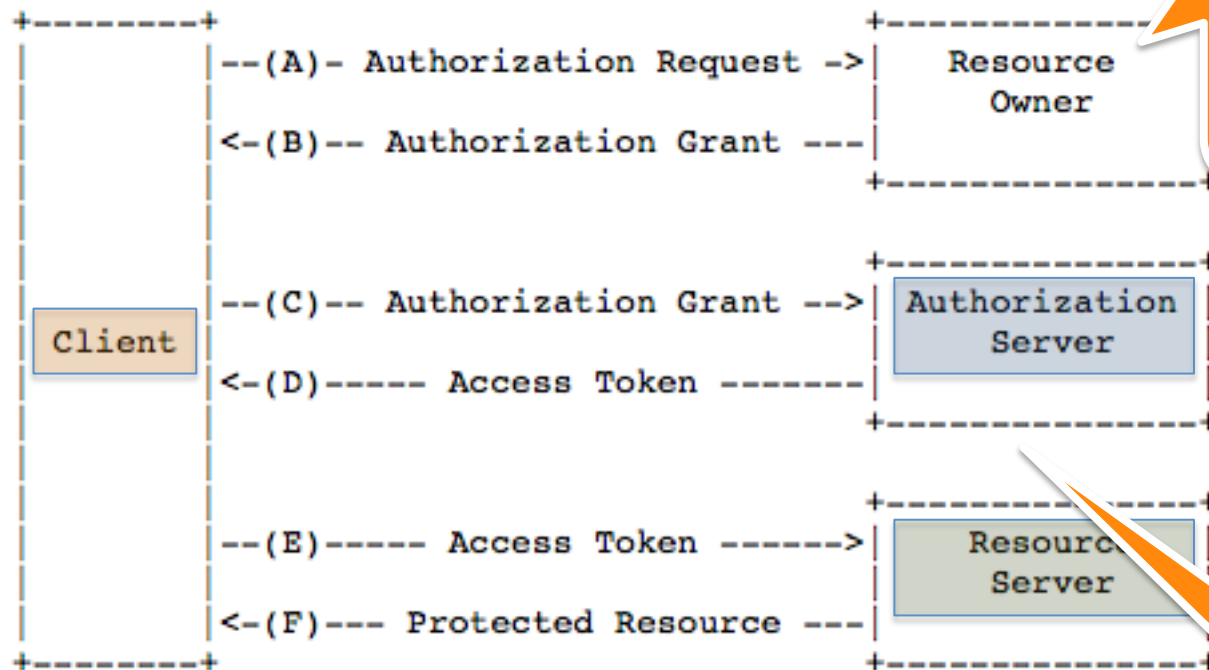
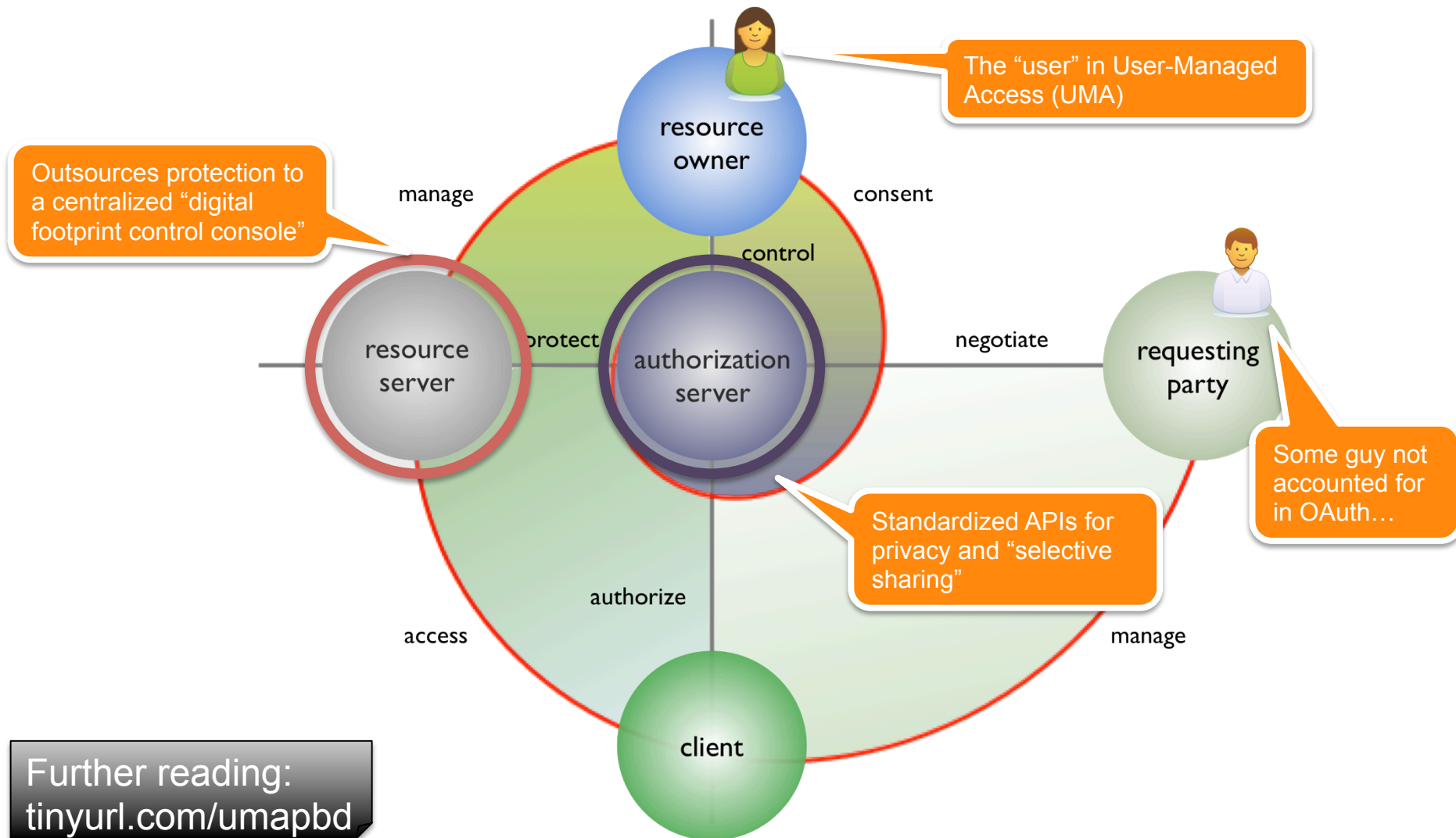


Figure 1: Abstract Protocol Flow

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

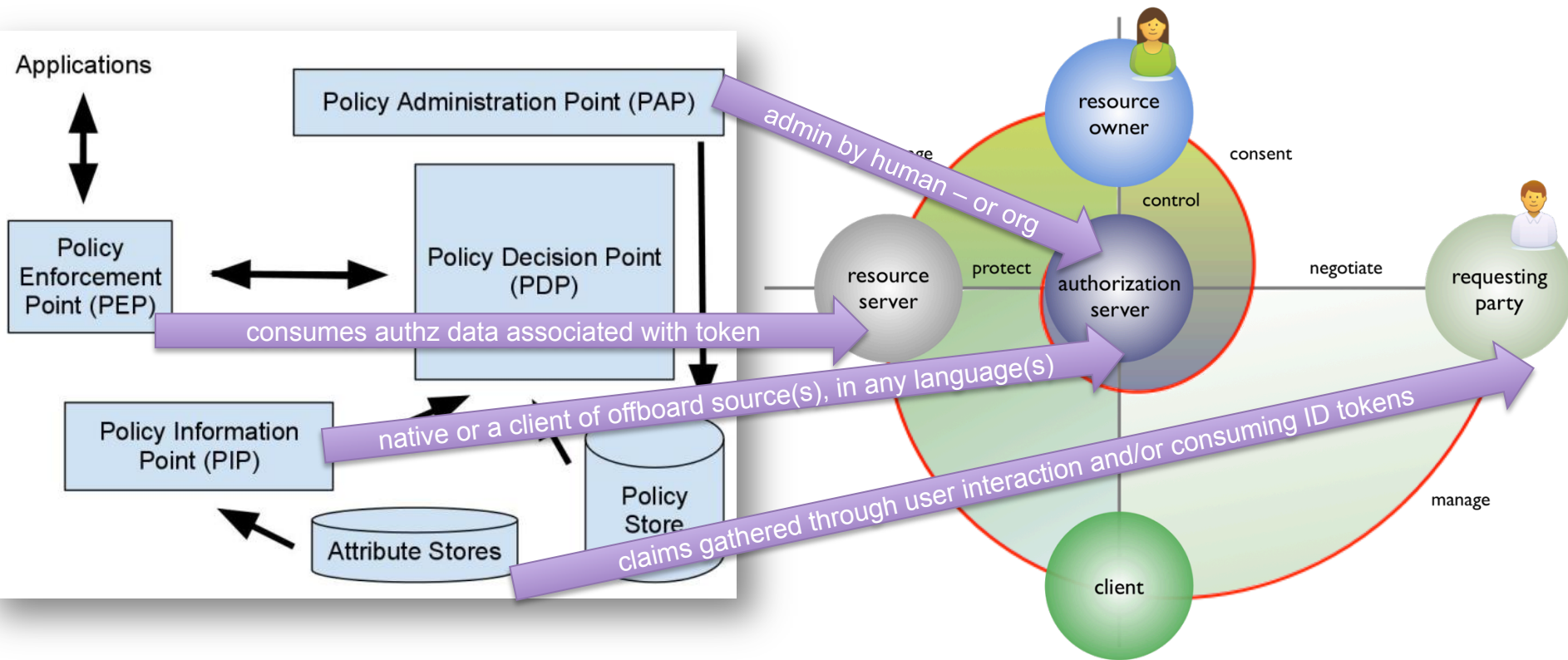
AS and RS are typically in the same domain and communicate in a proprietary way

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



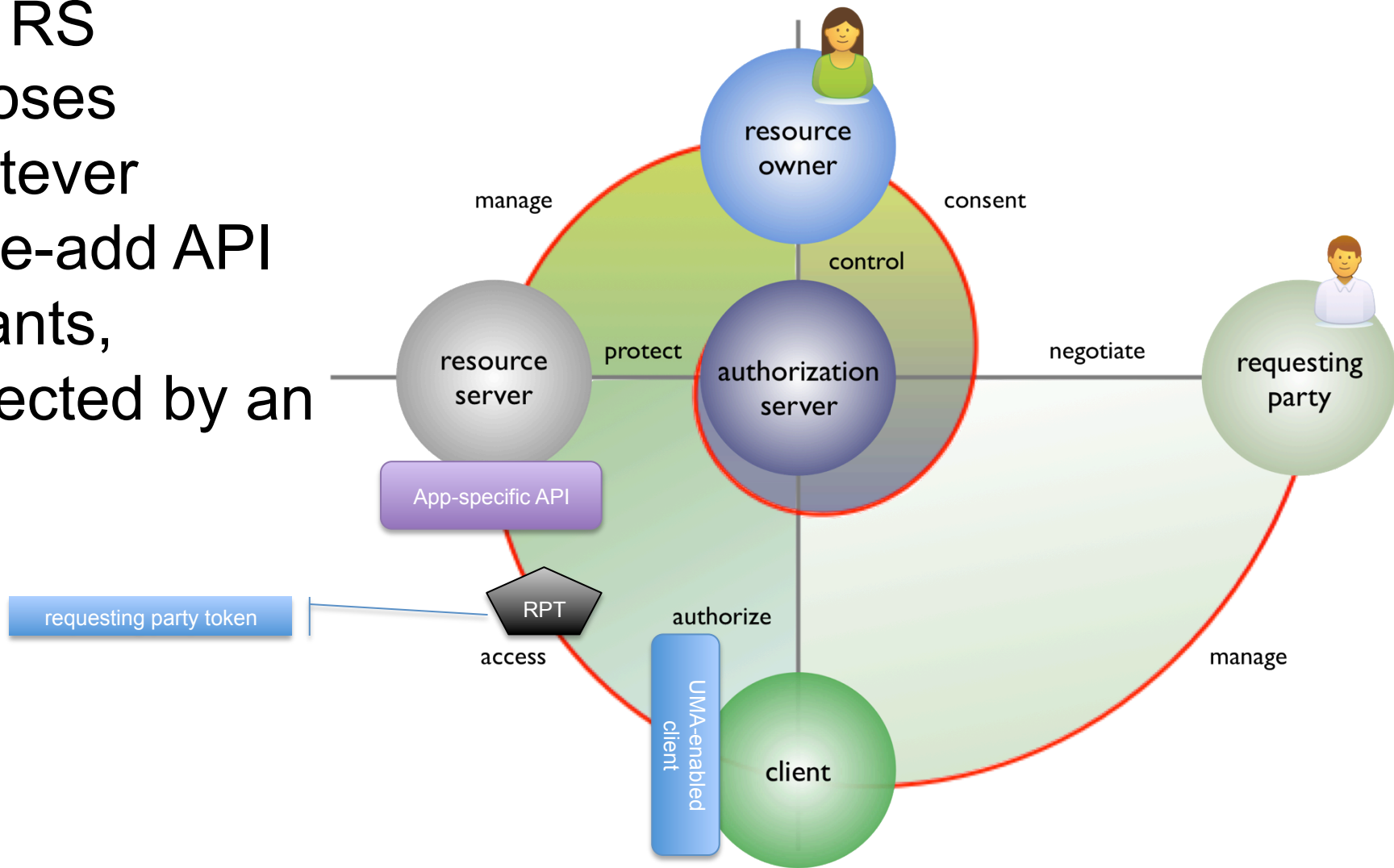
Further reading:
tinyurl.com/umapbd

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

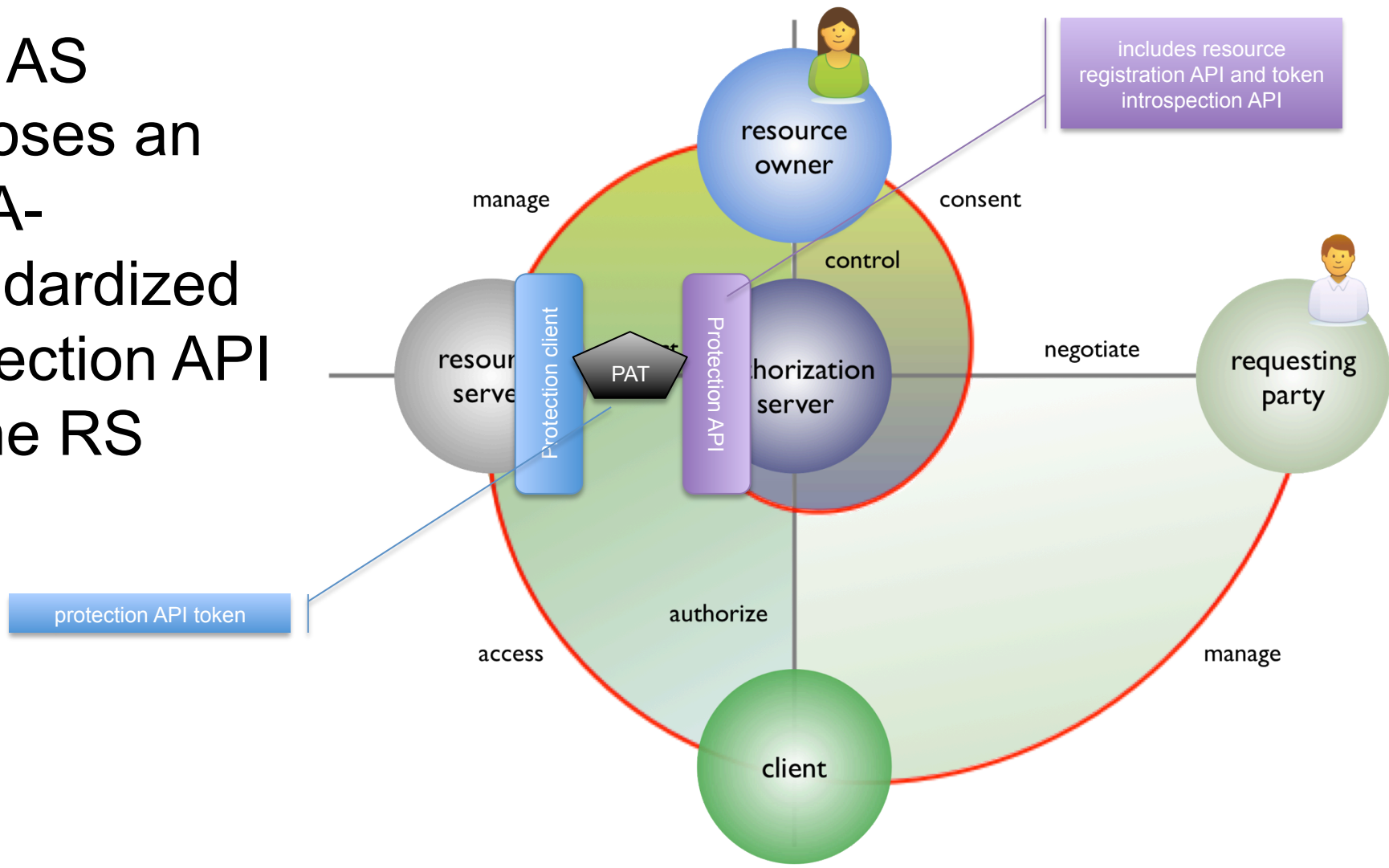


UMA and XACML can coexist nicely

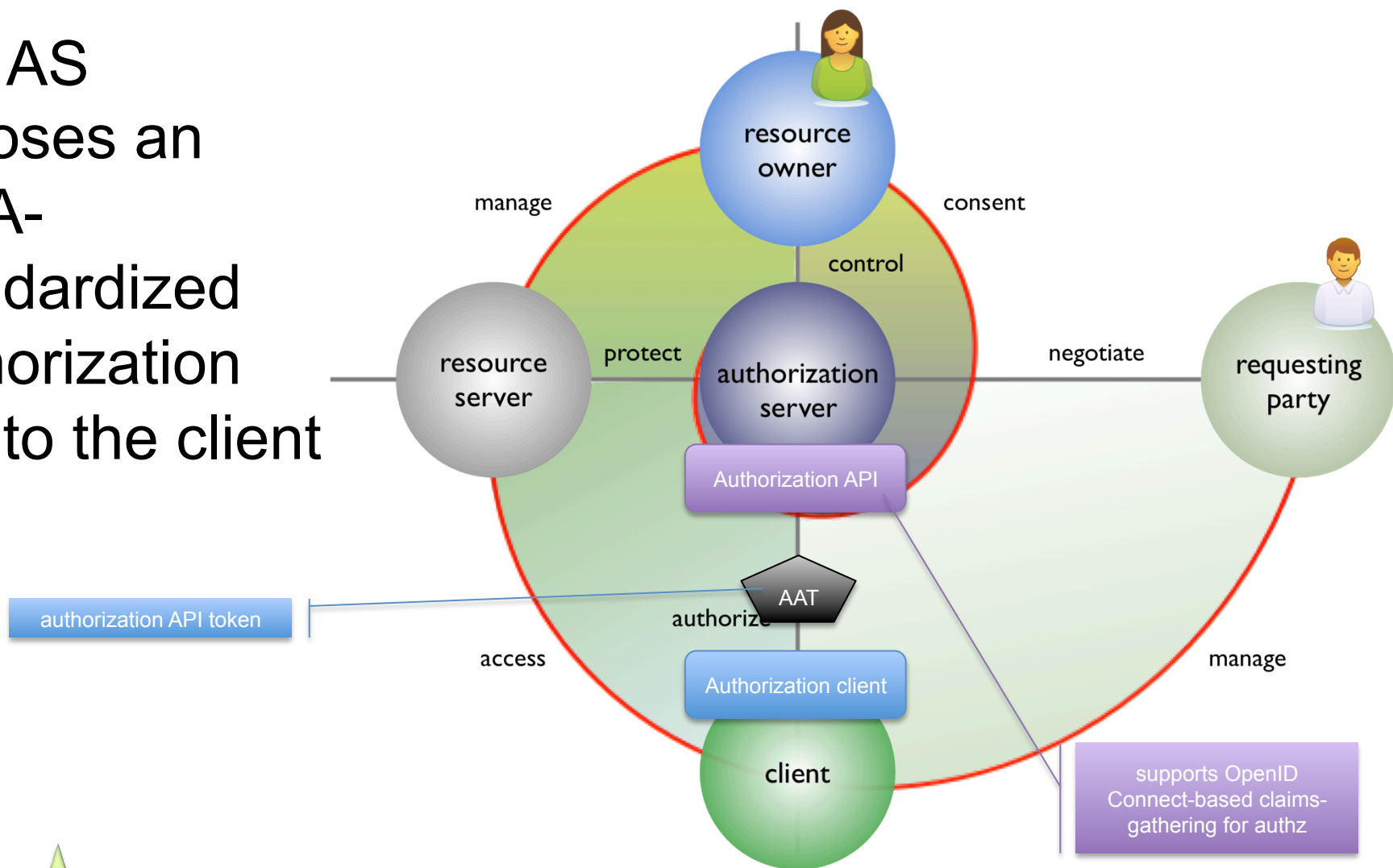
The RS exposes whatever value-add API it wants, protected by an AS



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



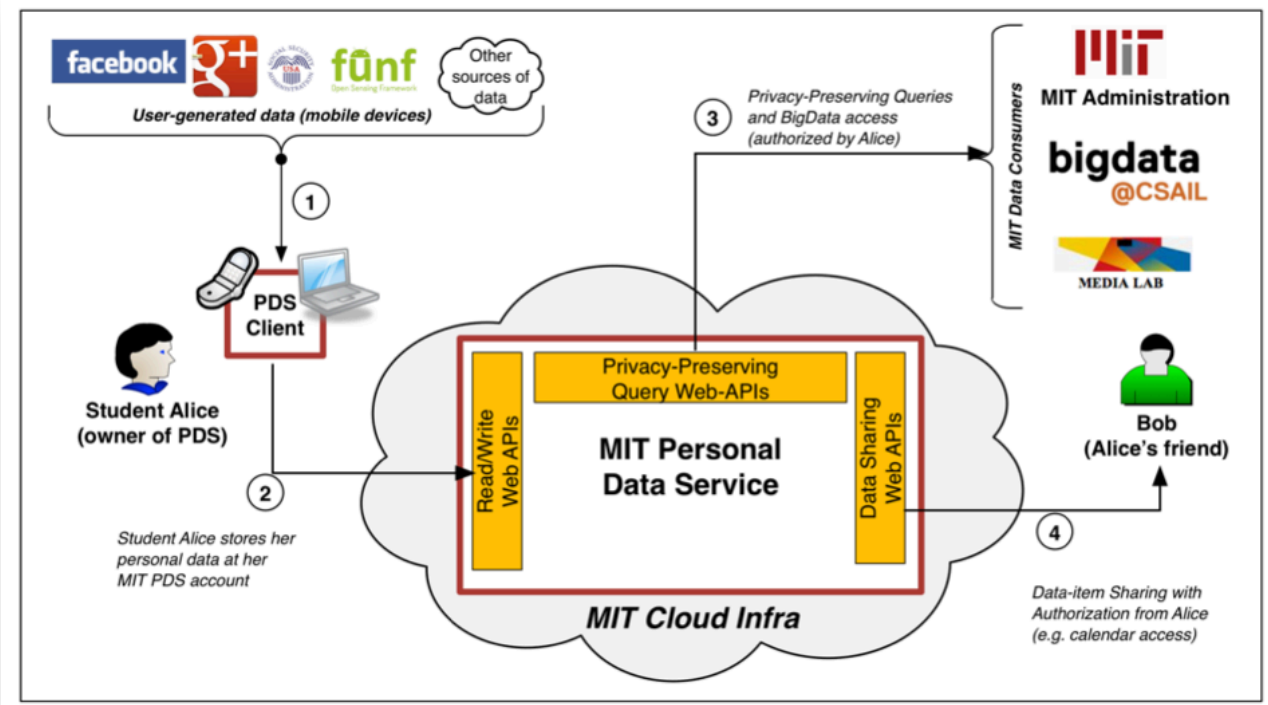
The AS exposes an UMA-standardized authorization API to the client



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



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"

Enterprise UMA case study

Further reading:
tinyurl.com/uma1iop

What vendors are saying and doing about UMA

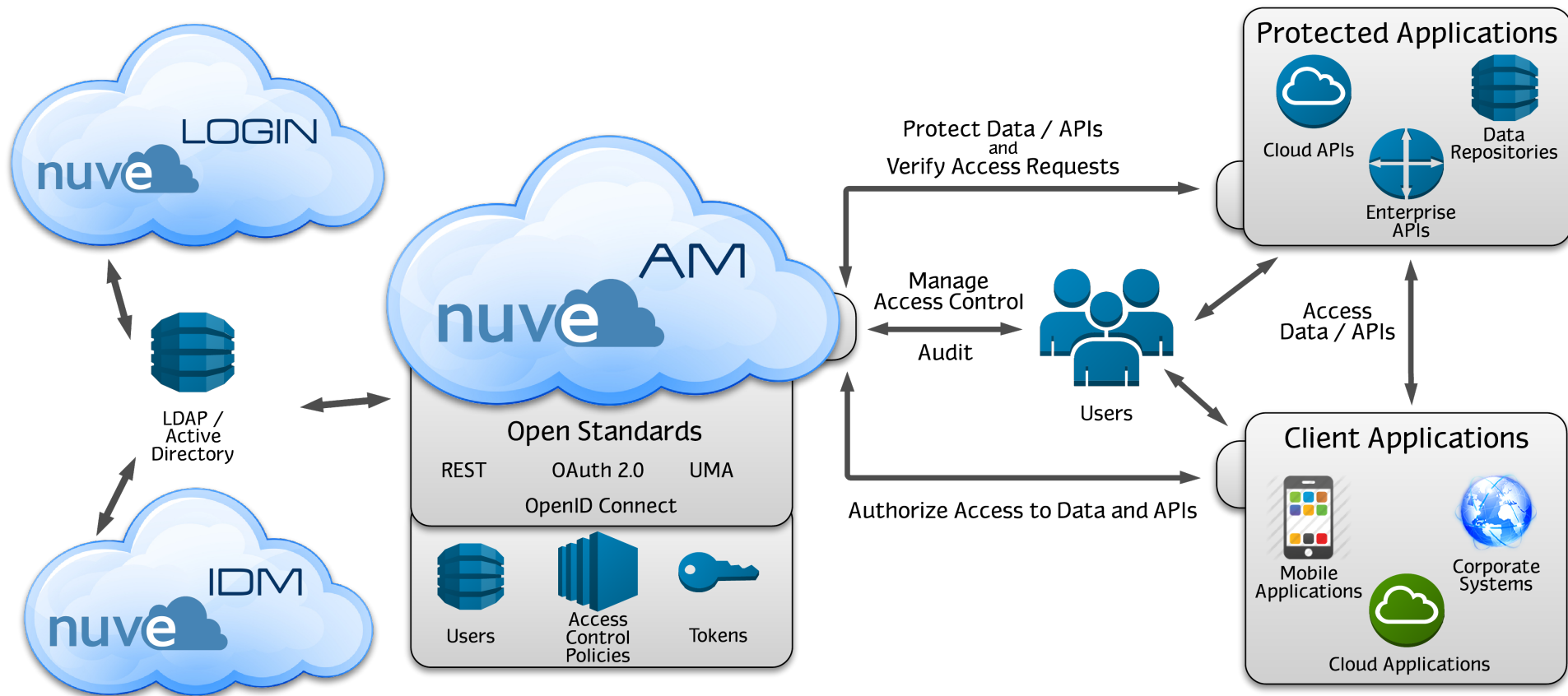
NuveAM by Cloud Identity

- 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



NuveAM for the enterprises

- 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 enterprises



Data



Contacts



Applications



History



Notifications

Home » History

Filter events: All / Authorizations / Resources / Policies



You added **James Martin (Minor Injuries Unit)** to sharing settings of **Chest X-Ray Images with comments**

18:45:40 19.03.2014 ([show details](#))



John Smith accessed **one of your resources** using **Minor Injuries Unit** application.

14:14:45 17.01.2014 ([show details](#))



John Smith accessed **one of your resources** using **Minor Injuries Unit** application.

14:14:45 17.01.2014 ([show details](#))



You accessed **Chest X-Ray Images with comments** using **Health Analysis App** application.



Resource name: Chest X-Ray Images with comments

Resource server: eHealth Vault

Requester: Health Analysis App

Access date: 14:14:45 17.01.2014

14:14:45 17.01.2014 ([hide details](#))

NuveAM for the enterprises

LOGIN Home **Settings** Sign In Widget Providers Configuration Analytics Create New App Application: demoapp Hi

Settings:

Application Info

Application Name:
demoapp

Application Login Domain:
demoapp.idfederate.com

Application API Key:
SjtxZTMkLf455O10gzDNUgFTBEyLATnvev86alMwUIURUXhXjuUJjQXID0rDMAv

Application Settings

Publish application:

Application icon URL: *

Save Changes

UMA Configuration

Enable UMA:

Client ID: PHiUVIDLPyczh8R0UfuacIU9IvN5ajxh1ro2XBvCHyfJOTKY8ieLR1Etu4PzNDhn

Client Secret: kmm3lOjl2nydGtWaOcDEMZwanD9HSDoqjiwTAX1CwijyvAWm2pKdGmolKFor201P

Redirect URL: *

Save Changes

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
- Stay tuned for another webinar in Q2

Join at:
tinyurl.com/umawg



Questions? Thank you!

@UMAWG

#UMAam20 *for questions*

20 March 2014

tinyurl.com/umawg *for slides, recording, and more*

