User-Managed Access (UMA) Working Group

Eve Maler, WG chair

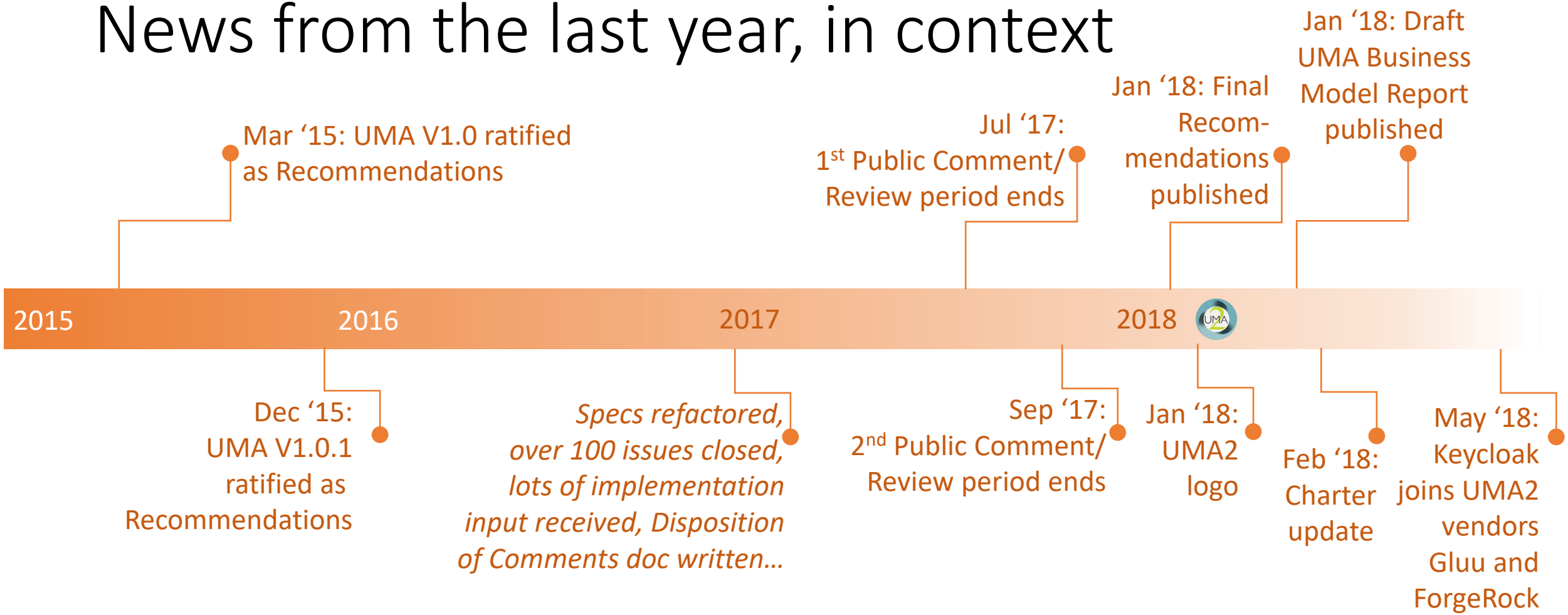
eve.maler@forgerock.com | @xmlgrrl

15 May 2018

http://tinyurl.com/umawg/ | @UMAWG

First: Shall we do an UMA explainer?

News from the last year, in context



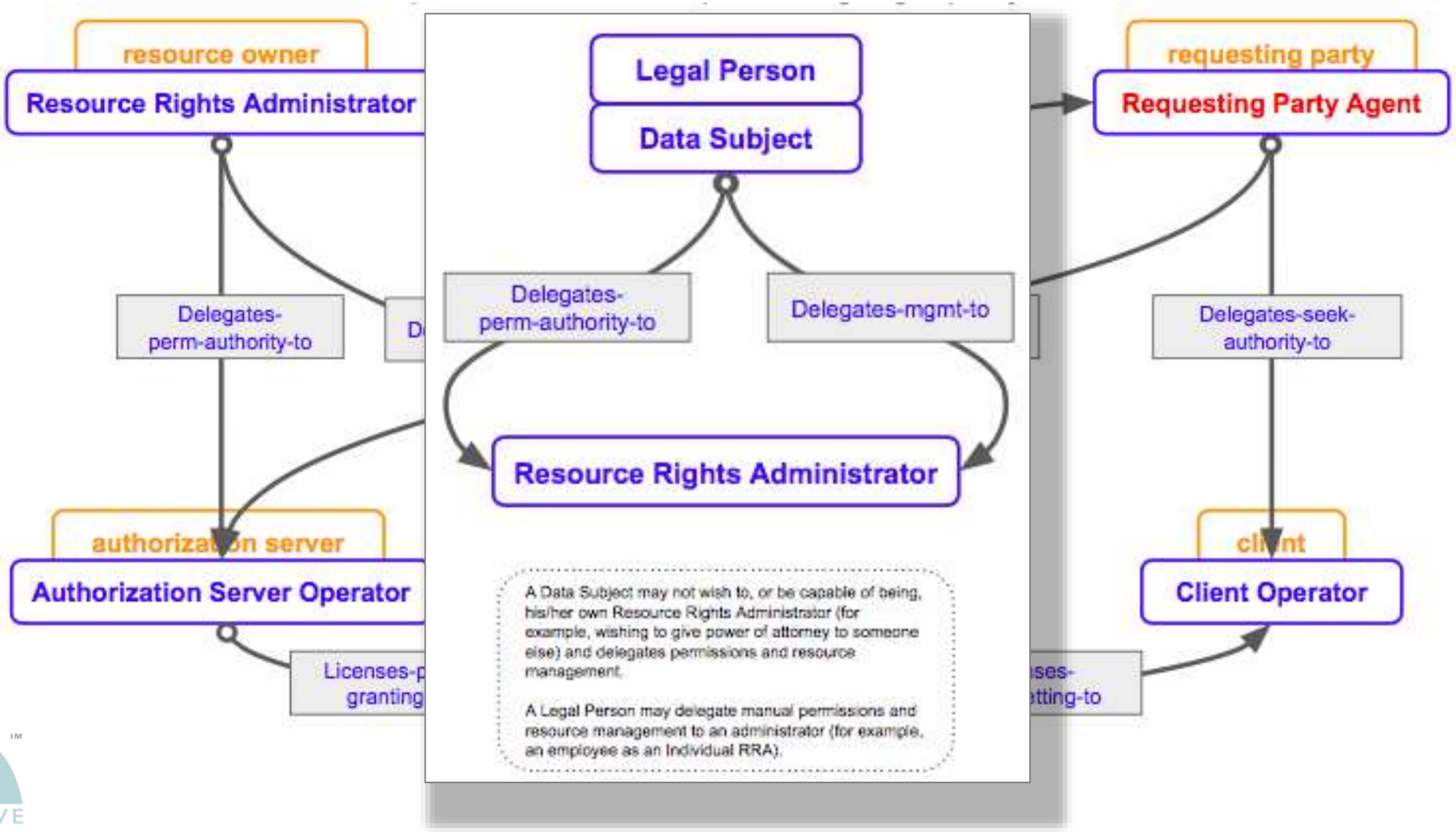
Some use cases/ecosystems involving UMA

- Financial
  - UK Pensions Dashboard Project / OIX / Origo
  - Examining suitability for a set of Open Banking use cases
- IoT
  - “ACE actors” architecture identifies requirements for authorization to an RqP
- Healthcare
  - Profiled in Health Relationship Trust (HEART) at OpenID Foundation
  - Part of the new OpenMedReady framework, along with HEART

kantara INITIATIVE™

UMA 2

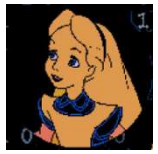
The UMA business model defines how the UMA protocol enables a license-based model for controlling access rights to personal digital assets



Key benefits of UMA to service providers

True security of delegated access

Scalability of resource permissioning



API-first protection strategy

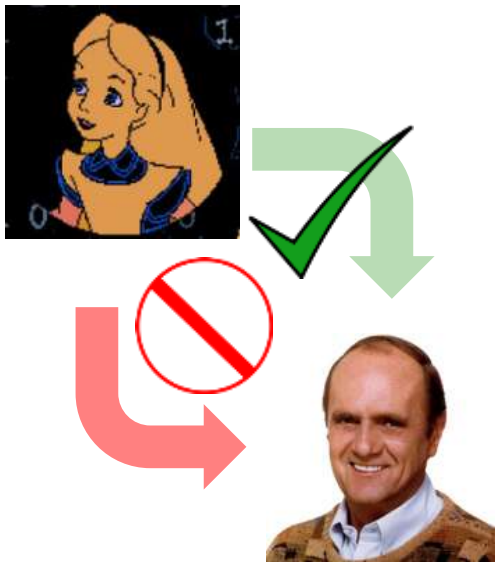
Fosters control for compliance and trust

kantara INITIATIVE™

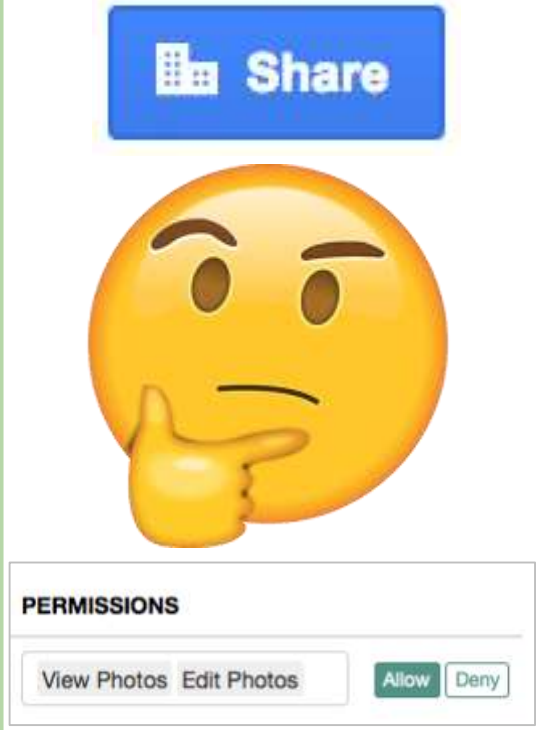
UMA

Key benefits of UMA to consumers

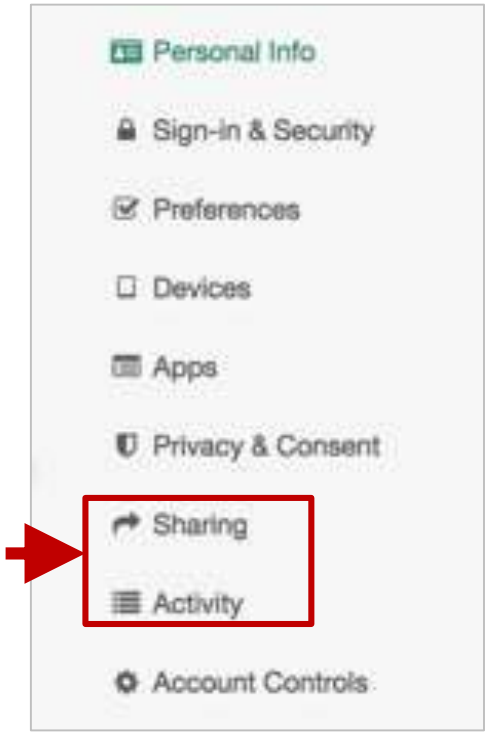
Constrained party-to-party delegation



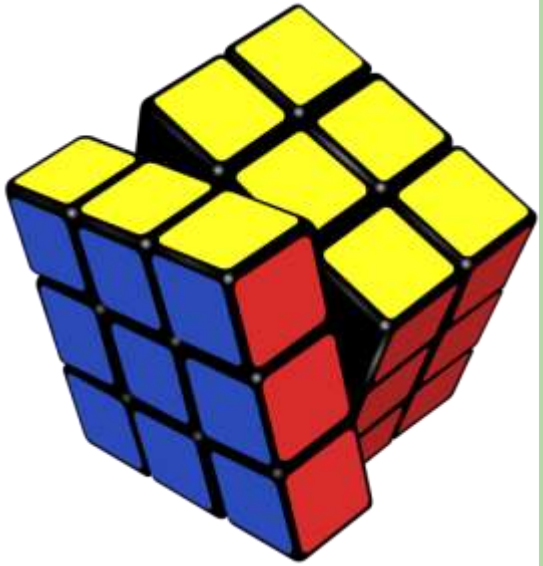
Granting consent without external influence



Centralized monitoring and management



Control of consents at a fine grain



kantara INITIATIVE™

UMA

OAuth, OIDC, and UMA2: breaking it down

OAuth is for constrained delegation to apps

It has helped to kill the “password anti-pattern”

Resource owner

Client

Authorization server

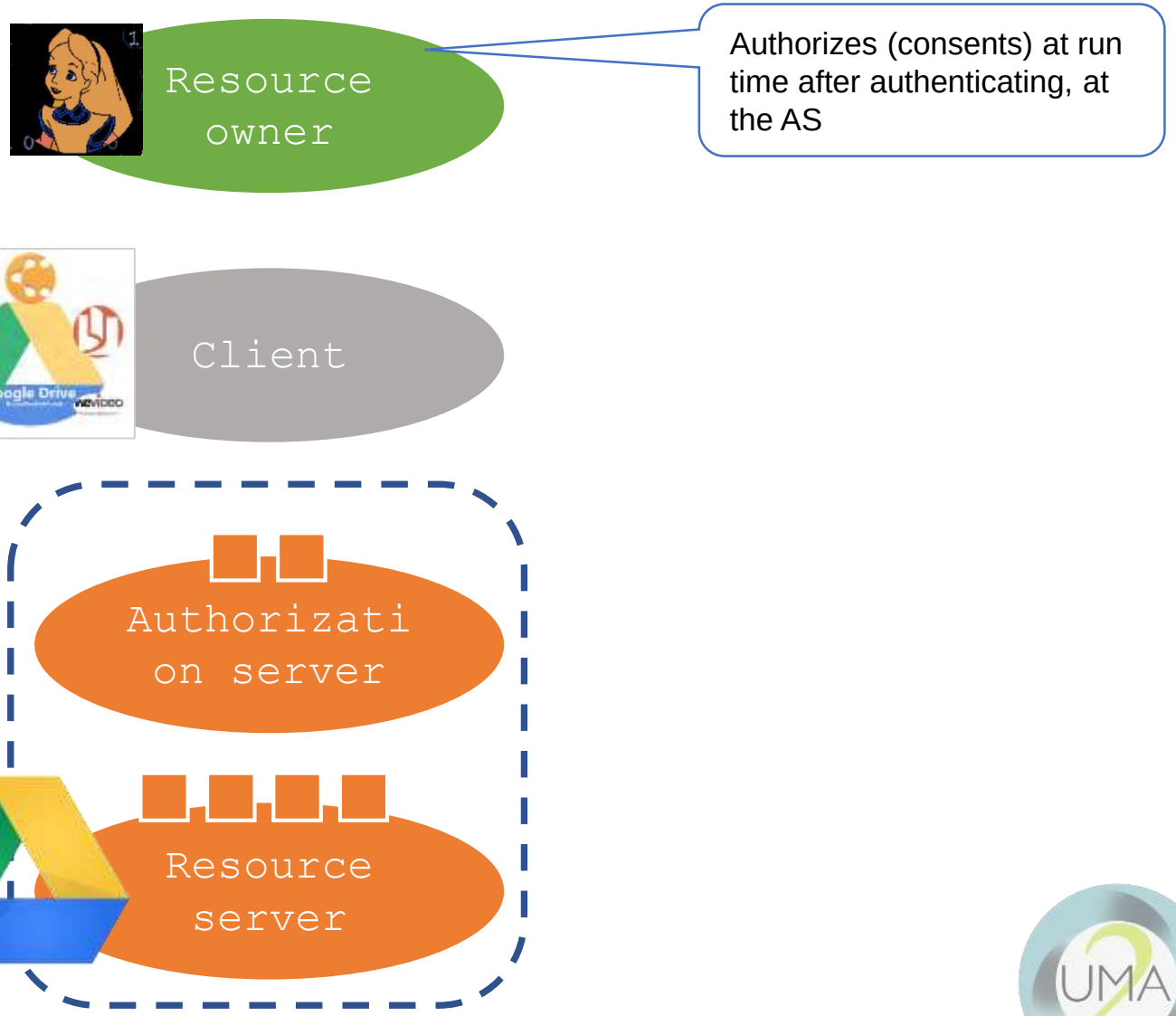
Resource server

kantara INITIATIVE™

UMA 2

OAuth is for constrained delegation to apps

It has helped to kill the “password anti-pattern”



OAuth is for constrained delegation to apps

It has helped to kill the “password anti-pattern”

Resource owner

Authorizes (consents) at run time after authenticating, at the AS

Client

App gets consent based on the API scopes it requested; it has its own identity distinct from the RO’s

Authorization server

Resource server

kantara INITIATIVE™

UMA 2

OAuth is for constrained delegation to apps

It has helped to kill the “password anti-pattern”

Resource owner

Authorizes (consents) at run time after authenticating, at the AS

Client

App gets consent based on the API scopes it requested; it has its own identity distinct from the RO’s

Authorization server

Standard OAuth endpoints for authorization and access token issuance

Resource server

kantara INITIATIVE™

UMA 2

OAuth is for constrained delegation to apps

It has helped to kill the “password anti-pattern”

Resource owner

Authorizes (consents) at run time after authenticating, at the AS

Client

App gets consent based on the API scopes it requested; it has its own identity distinct from the RO’s

Authorization server

Standard OAuth endpoints for authorization and access token issuance

Resource server

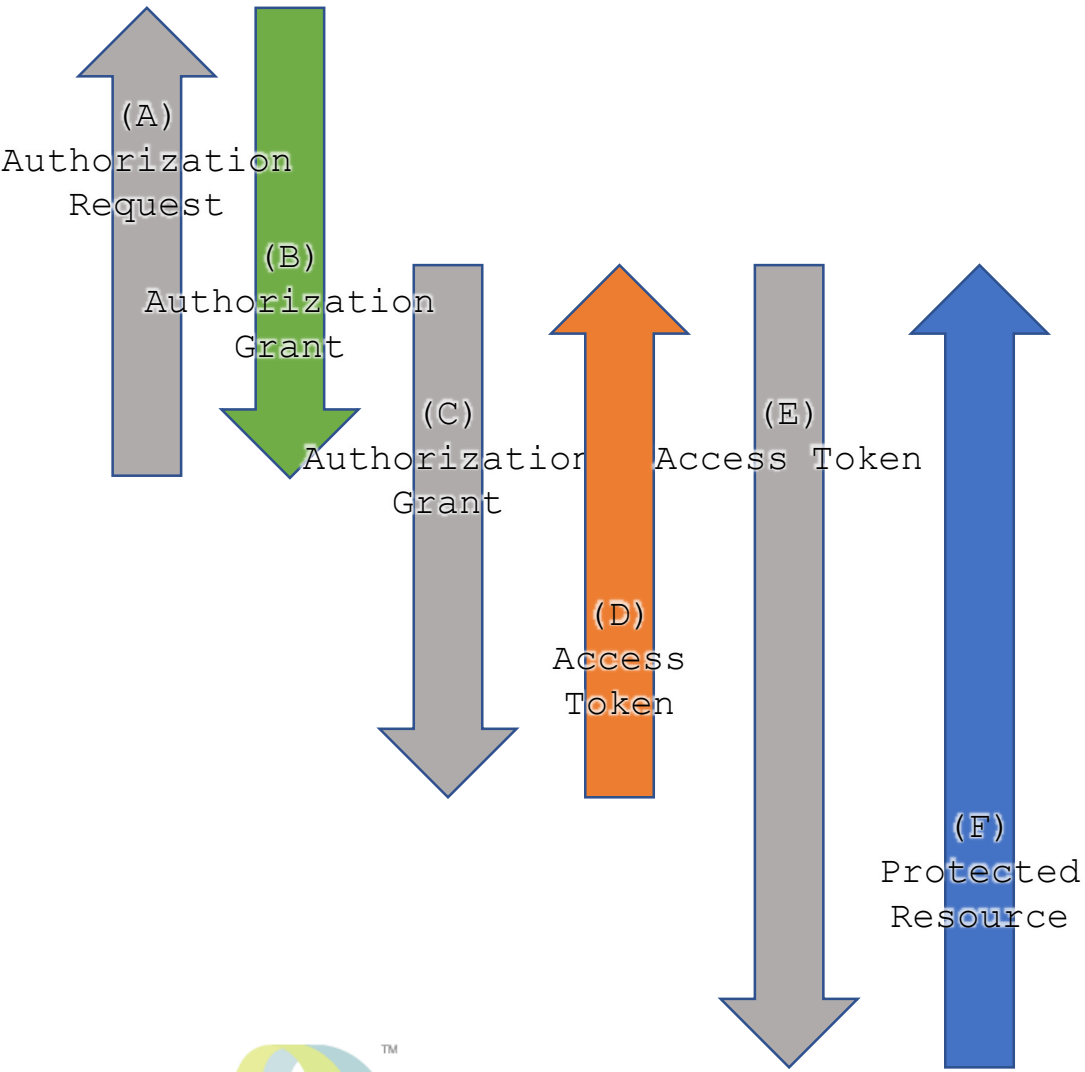
Some number of API endpoints that deliver the data or other value-add

kantara INITIATIVE

UMA 2

OAuth is for constrained delegation to apps

It has helped to kill the “password anti-pattern”



Resource owner

Authorizes (consents) at run time after authenticating, at the AS

Client

App gets consent based on the API scopes it requested; it has its own identity distinct from the RO’s

Authorization server

Standard OAuth endpoints for authorization and access token issuance

Resource server

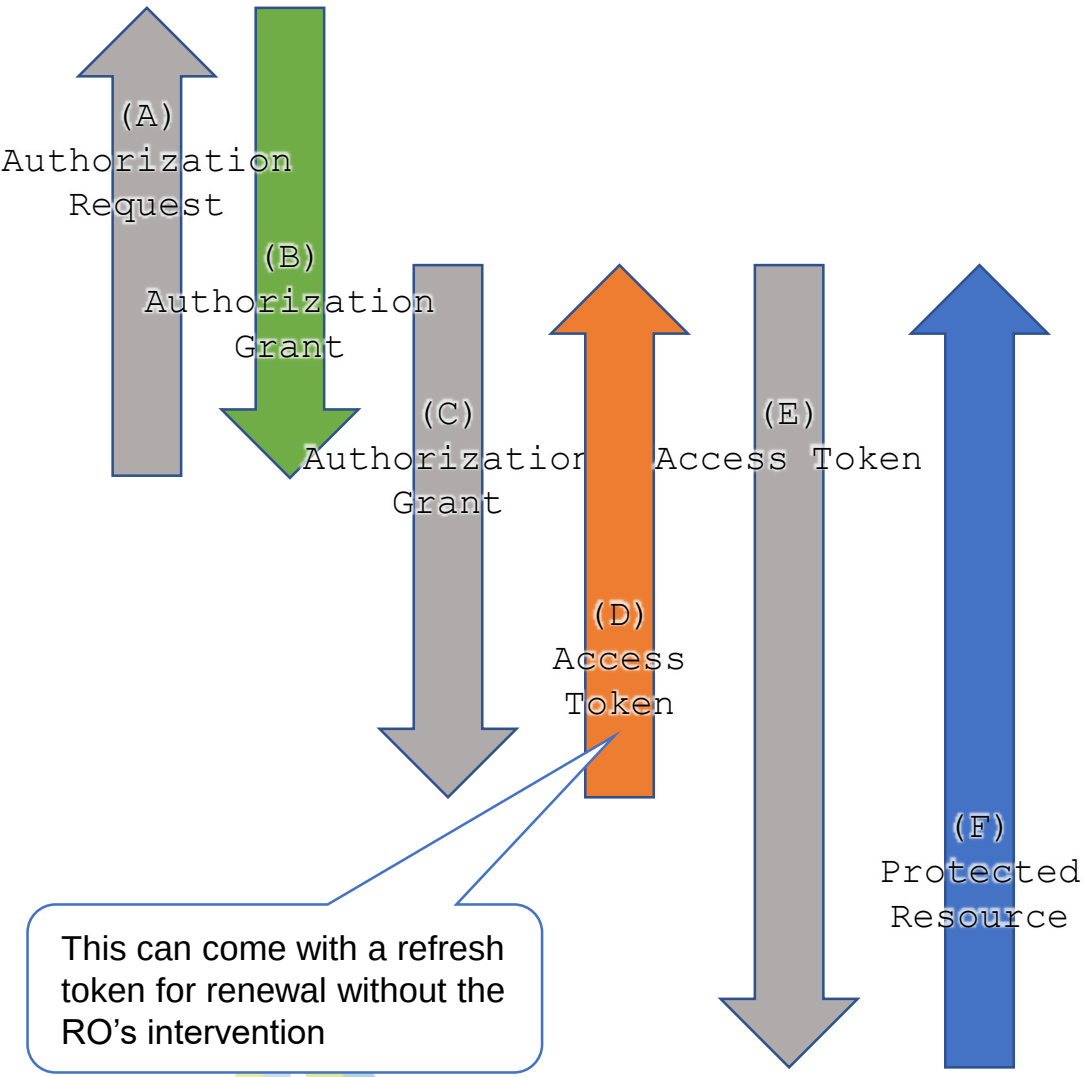
Some number of API endpoints that deliver the data or other value-add

kantara INITIATIVE

UMA 2

OAuth is for constrained delegation to apps

It has helped to kill the “password anti-pattern”



Resource owner

Authorizes (consents) at run time after authenticating, at the AS

Client

App gets consent based on the API scopes it requested; it has its own identity distinct from the RO’s

Authorization server

Standard OAuth endpoints for authorization and access token issuance

Resource server

Some number of API endpoints that deliver the data or other value-add

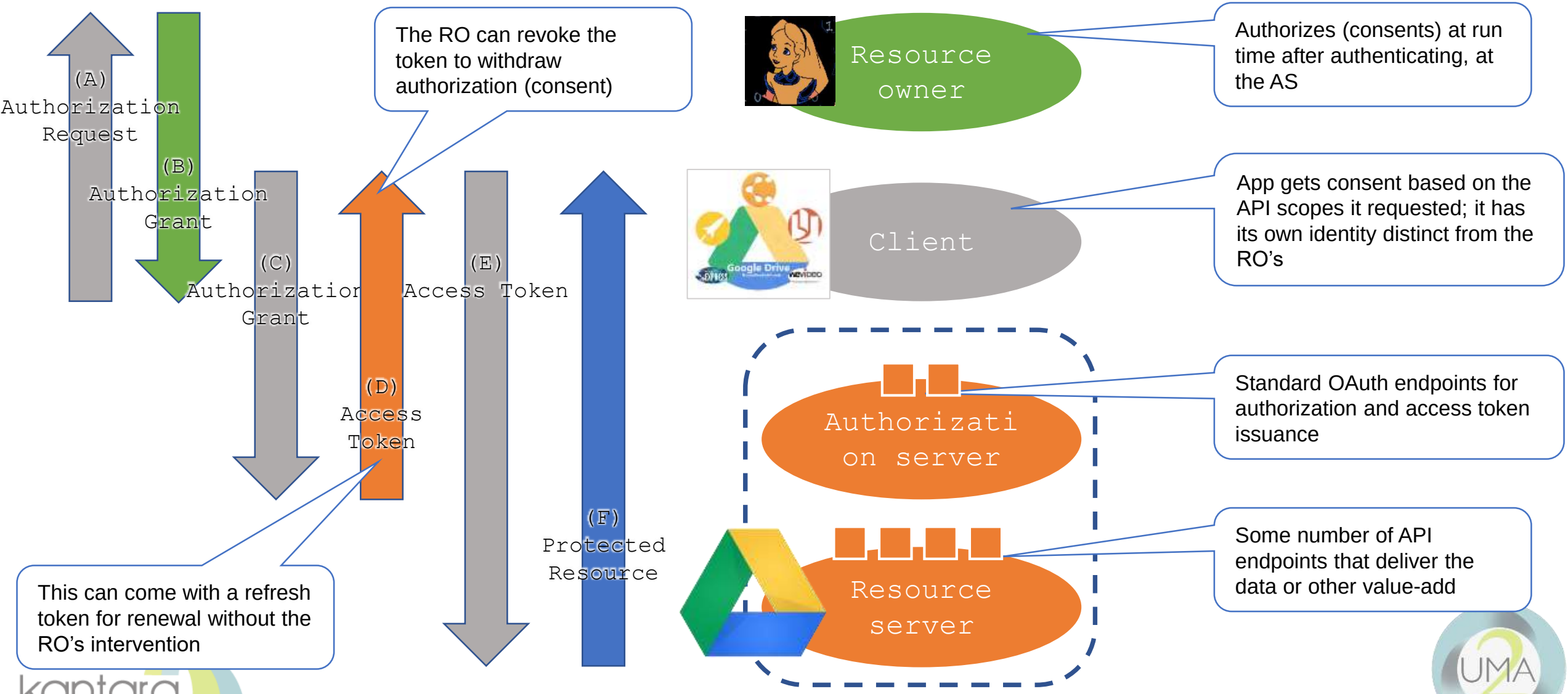
This can come with a refresh token for renewal without the RO’s intervention

kantara INITIATIVE

UMA 2

OAuth is for constrained delegation to apps

It has helped to kill the “password anti-pattern”



kantara INITIATIVE

UMA 2

OpenID Connect does modern-day federation

It is an OAuth-protected identity API, plus a bit more

Resource owner

Client

Authorization server

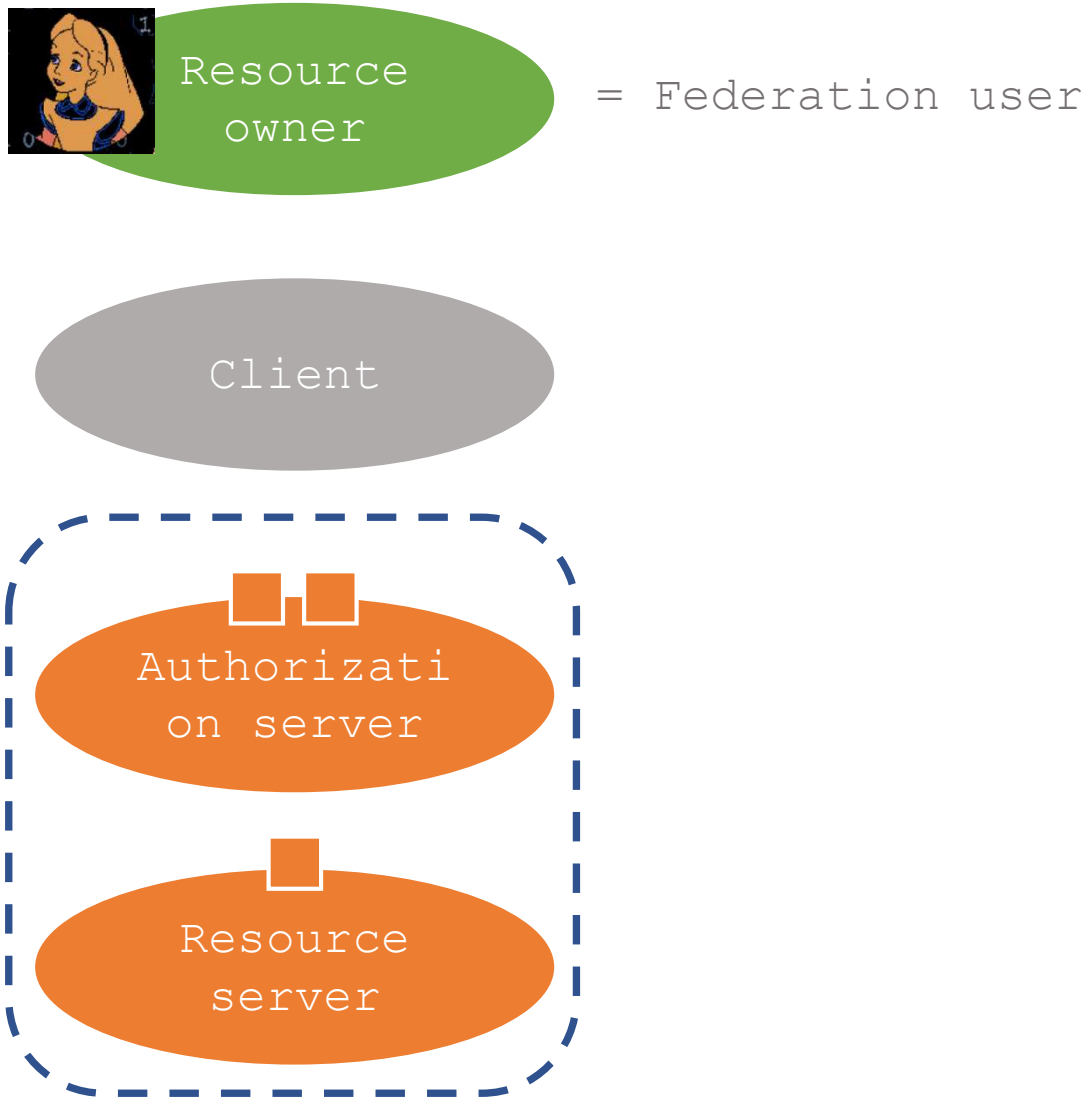
Resource server

kantara INITIATIVE™

UMA 2

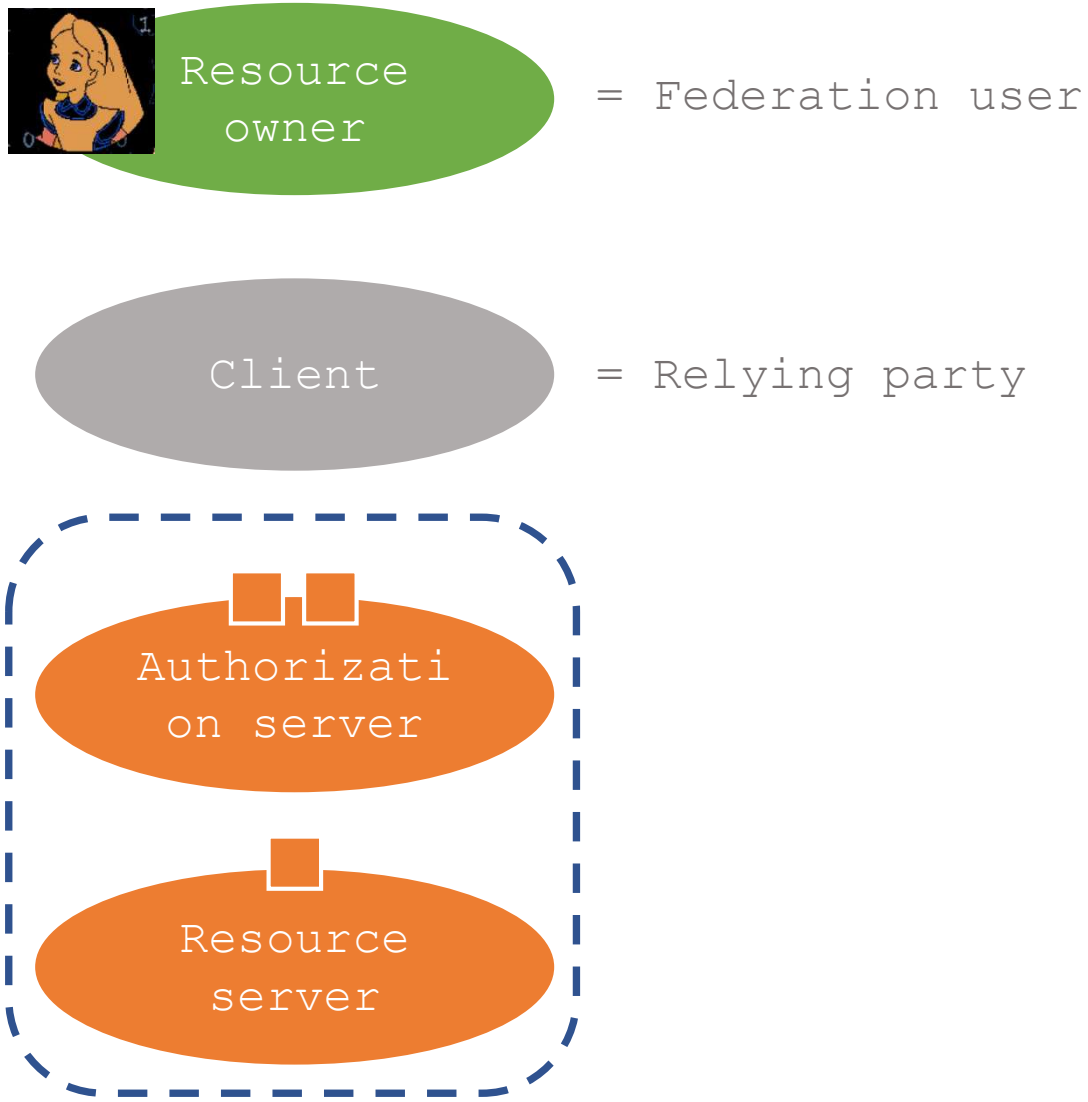
OpenID Connect does modern-day federation

It is an OAuth-protected identity API, plus a bit more



OpenID Connect does modern-day federation

It is an OAuth-protected identity API, plus a bit more



OpenID Connect does modern-day federation

It is an OAuth-protected identity API, plus a bit more

Resource owner

= Federation user

Client

= Relying party

Authorization server

Resource server

= Identity provider
("OpenID provider")

kantara INITIATIVE

UMA 2

OpenID Connect does modern-day federation

It is an OAuth-protected identity API, plus a bit more

Resource owner

= Federation user

Client

= Relying party

Token endpoint typically delivers an “ID token” similar to a SAML assertion

Authorization server

Resource server

= Identity provider
(“OpenID provider”)

kantara INITIATIVE™

UMA 2

OpenID Connect does modern-day federation

It is an OAuth-protected identity API, plus a bit more

Resource owner

= Federation user

Client

= Relying party

Token endpoint typically delivers an “ID token” similar to a SAML assertion

Authorization server

Standard UserInfo endpoint can be called with an access token to look up identity claims

Resource server

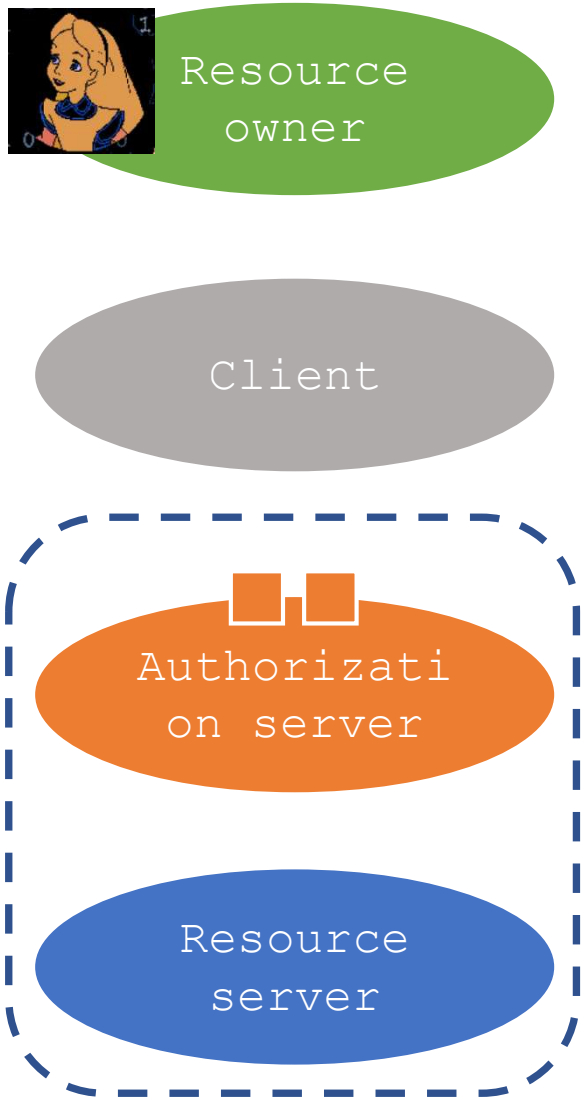
= Identity provider (“OpenID provider”)

kantara INITIATIVE

UMA 2

User-Managed Access is for cross-party sharing

UMA brings next-gen delegation and consent to OAuth



User-Managed Access is for cross-party sharing

UMA brings next-gen delegation and consent to OAuth

Resource owner

Requesting party

Client

Authorization server

Resource server

kantara INITIATIVE™

UMA 2

User-Managed Access is for cross-party sharing

UMA brings next-gen delegation and consent to OAuth

Resource owner

Requesting party

Client

Authorization server

Resource server

kantara INITIATIVE™

UMA 2

User-Managed Access is for cross-party sharing

UMA brings next-gen delegation and consent to OAuth

Resource owner

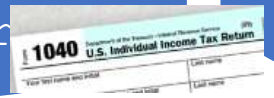
Requesting party

Client

Authorization server

Resource server

Resource server



Resource server

kantara INITIATIVE

UMA 2

User-Managed Access is for cross-party sharing

UMA brings next-gen delegation and consent to OAuth

Resource owner

Requesting party

At run time

UX

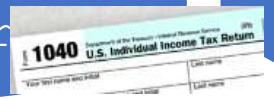
Opt in

Client

Authorization server

Resource server

Resource server



Resource server

kantara INITIATIVE

UMA 2

User-Managed Access is for cross-party sharing

UMA brings next-gen delegation and consent to OAuth

Resource owner

Requesting party

Ahead of time

At run time

UX

Share

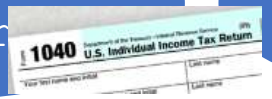
Opt in

Client

Authorization server

Resource server

Resource server



Resource server

kantara INITIATIVE

UMA 2

User-Managed Access is for cross-party sharing

UMA brings next-gen delegation and consent to OAuth

Resource owner

Requesting party

Ahead of time

At run time

After the fact

UX

Share

Opt in

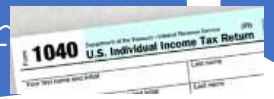
Approve

Client

Authorization server

Resource server

Resource server



Resource server

kantara INITIATIVE

UMA 2

User-Managed Access is for cross-party sharing

UMA brings next-gen delegation and consent to OAuth

Resource owner

Requesting party

Ahead of time | Anytime | At run time | After the fact

UX

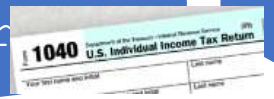
Share | Monitor | Opt in | Approve

Client

Authorization server

Resource server

Resource server



Resource server

kantara INITIATIVE

UMA 2

User-Managed Access is for cross-party sharing

UMA brings next-gen delegation and consent to OAuth

Resource owner

Requesting party

Ahead of time | Anytime | Anytime | At run time | After the fact

UX

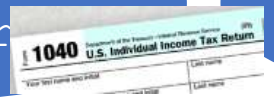
Share | Monitor | Withdraw | Opt in | Approve

Client

Authorization server

Resource server

Resource server



Resource server

kantara INITIATIVE

UMA 2

Questions?
Thank you!
Join us!

Eve Maler, WG chair

eve.maler@forgerock.com| @xmlgrrl

15 May 2018

http://tinyurl.com/umawg/ | @UMAWG