Applications on the Edge of the OAuth Standards Wave

Dan Blum
Senior Analyst
KuppingerCole
db@kuppingercole.com

Pam Dingle
Director of Identity Standards
Microsoft
@pamelarosiedee

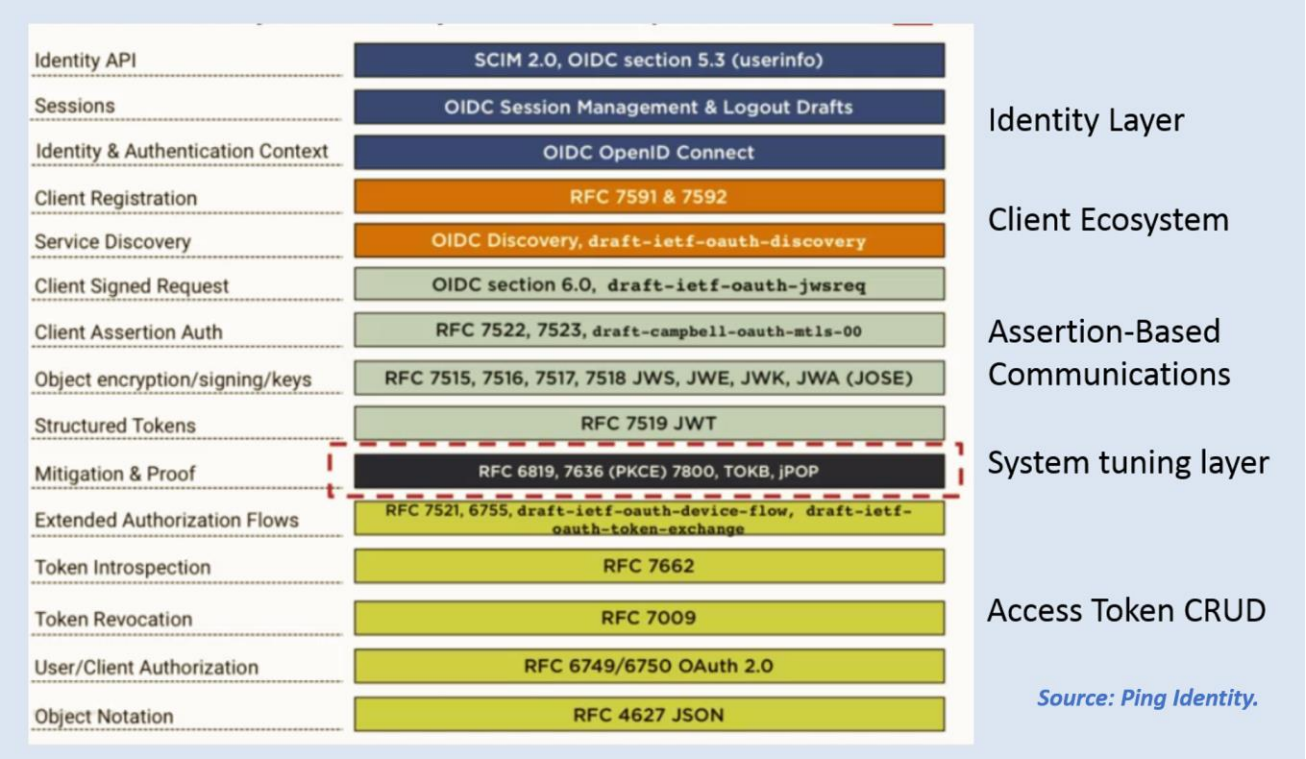
eiC 2018
12TH EUROPEAN IDENTITY & CLOUD CONFERENCE

Thursday, 17.05.2018

KC Agenda

Part 1 Dan Blum	Introduction to OAuth and the new standards stack
Part 2 Pam Dingle	Examples and good practices based on implementation experience and customer use cases
Part 3	Audience questions welcome

OAuth Standards Stack



kuppingercole ANALYSTS

Menu View

Appetizers

User AuthN
Client AuthN
Assertion formats

Sides

Access token
CRUD
Introspection

Drinks

UX
UMA,
Consent
Receipts

Entrees

OAuth 2.0
Provisioning
Client Ecosystems

Desserts

Device flows
Session management

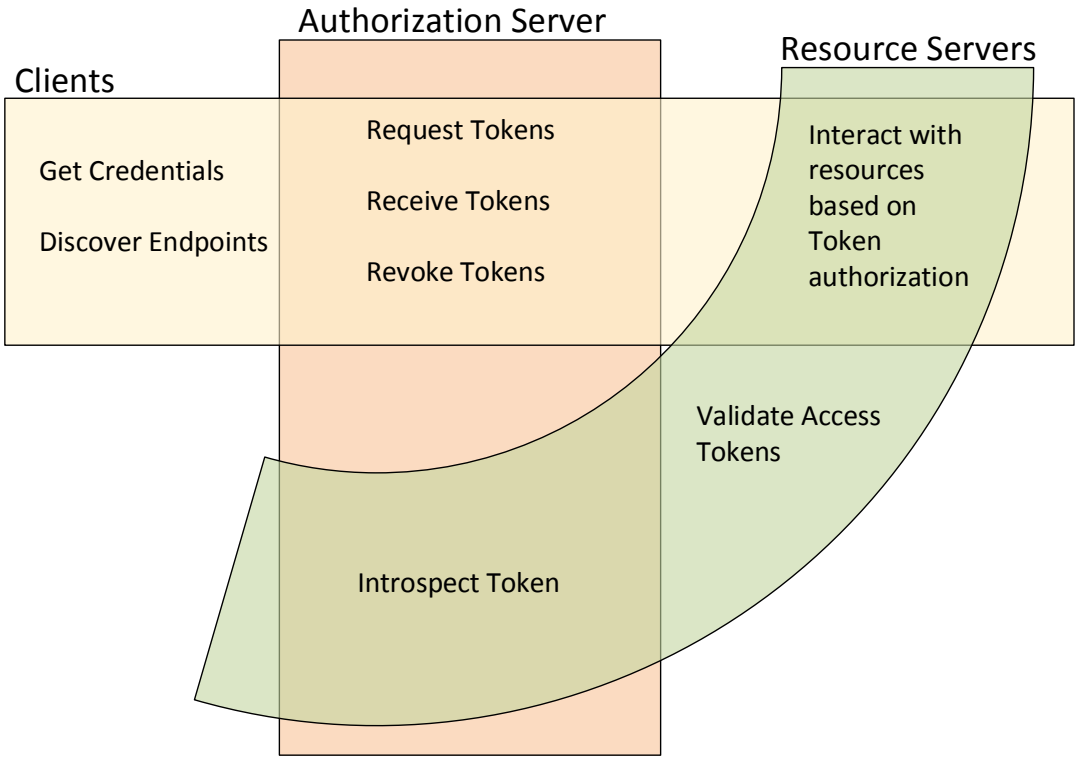
Prep instructions: System Tuning

Refresher Course on OAuth

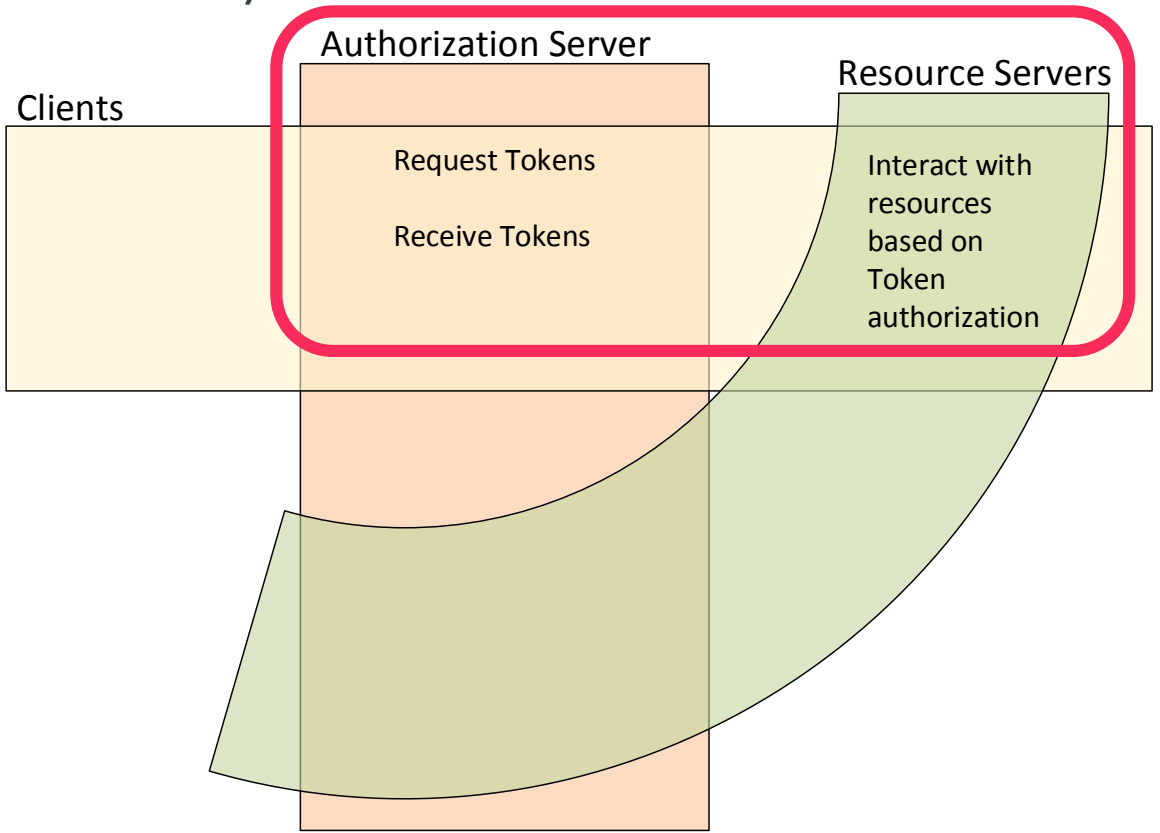
- OAuth 2.0 is a very important IETF specification(s)
  - Used with many of > 7,000 APIs listed on the http://programmableweb.com site
  - Models the interactions between a user, client, authorization server, and resource server
  - Supports four flows
    - Authorization Code Grant
    - Implicit Grant
    - Resource Owner Password Credentials Grant
    - Client Credentials Grant

See Oauth 2.0 Simplified for more information

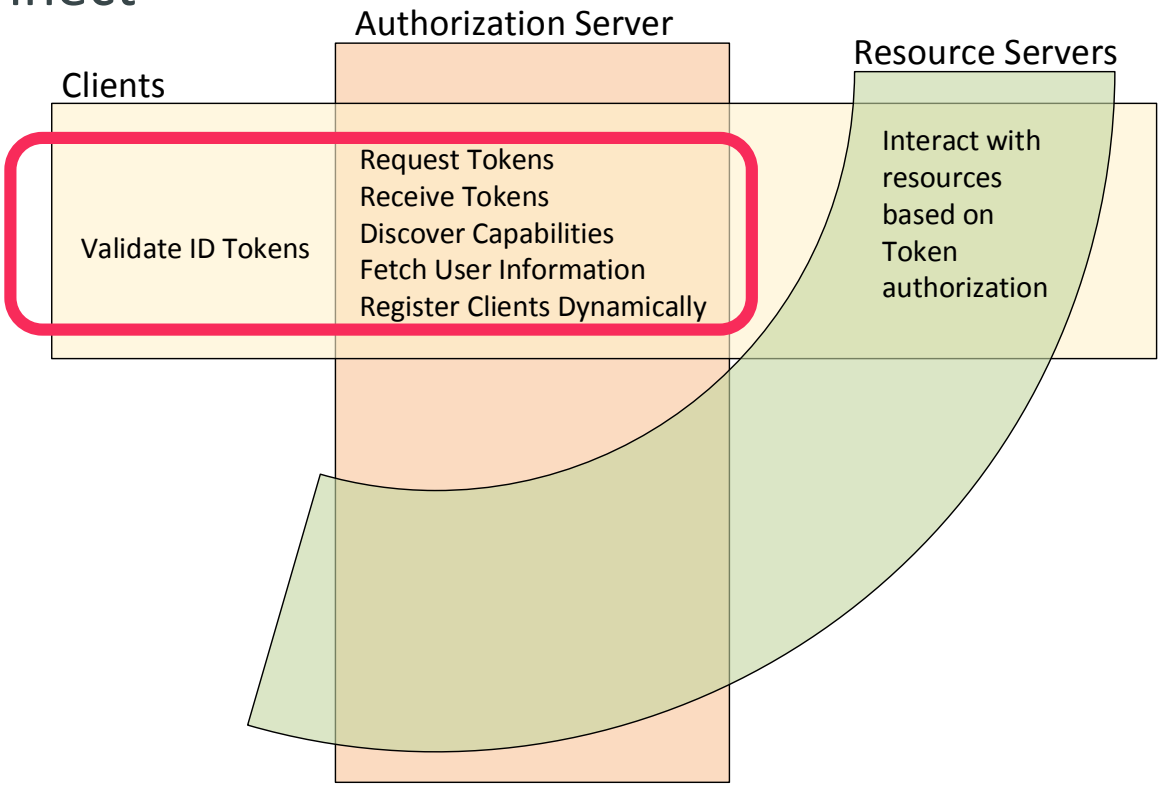
Token Ecosystems for API Security



RFC 6749/50 (OAuth 2.0)



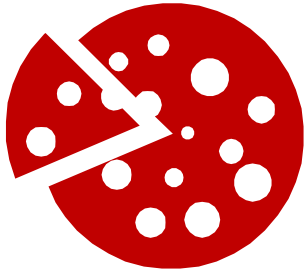
OpenID Connect

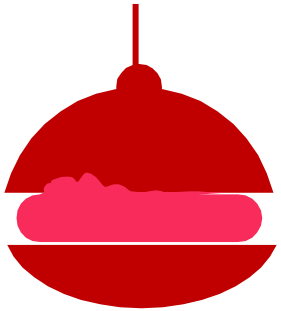


kuppingercole ANALYSTS

eic 2018 12TH EUROPEAN IDENTITY & CLOUD CONFERENCE

Entrees

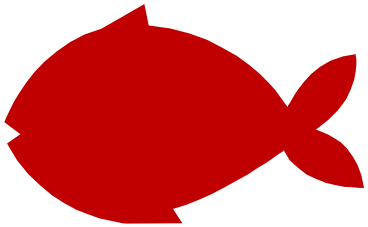




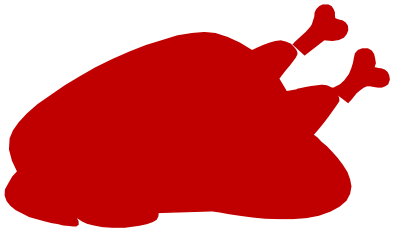
OAuth 2.0
User/client
Authorization

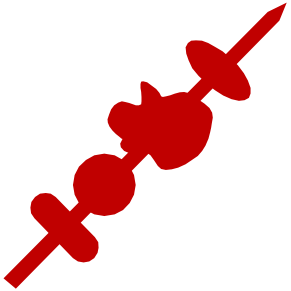
Provisioning
Automate
Onboarding
Improve
control

Client Ecosystems
Registration
Service
discovery



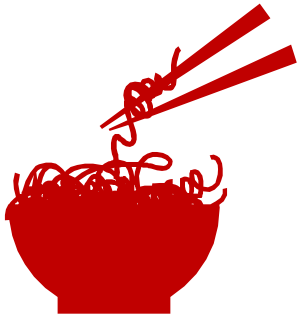
- Examples and good practices

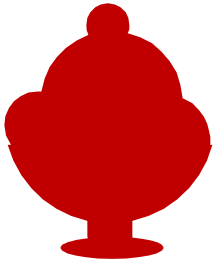




Authentication Methods

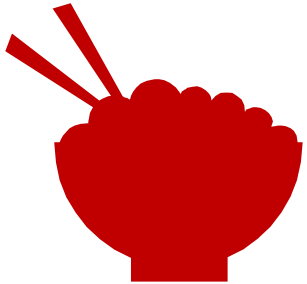
- Authentication may out of scope for OAuth, but it's hardly out of scope for the user experience!
  - Using OpenID Connect in conjunction with OAuth
  - Federating additional assertion formats to OAuth
- Examples and good practices





Access Token CRUD

- Create, read, update, delete (or revoke)
- Token introspection
- Examples and good practices

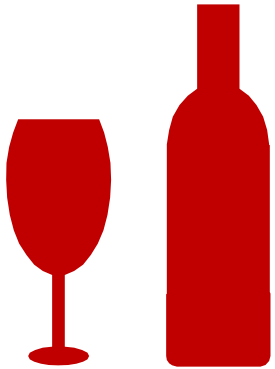


Desserts

- Device flows
- Session management
- Examples and good practices

Drinks

- User experience
- User Managed Access (UMA)
- Consent receipts
- Examples and good practices



System Tuning

- Token bindings
- Profiles
- Certification
- Examples and good practices

OAuth-Based Identity Standards Glossary

IETF REQUEST FOR COMMENTS (RFCs) – 1 of 2

RFC6749 The OAuth 2.0 Authorization Framework. D. Hardt, Ed.. October 2012.
RFC6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage. M. Jones,D. Hardt. October 2012
RFC6755 An IETF URN Sub-Namespace for OAuth. B. Campbell, H. Tschofenig. October 2012.
RFC6819 OAuth 2.0 Threat Model and Security Considerations. T. Lodderstedt, Ed., M. McGloin, P. Hunt. January 2013.
RFC7009 OAuth 2.0 Token Revocation. T. Lodderstedt, Ed., S. Dronia, M. Scurtescu. August 2013.
RFC7521 Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants. B. Campbell, C. Mortimore, M. Jones, Y.Goland. May 2015.
RFC7522 Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants. B. Campbell, C. Mortimore, M. Jones. May 2015.
RFC7523 JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants. M. Jones, B. Campbell, C. Mortimore. May 2015.

OAuth-Based Identity Standards Glossary

IETF REQUEST FOR COMMENTS (RFCs) – 2 of 2

RFC7591 OAuth 2.0 Dynamic Client Registration Protocol. J. Richer, Ed., M. Jones, J. Bradley, M. Machulak, P. Hunt. July 2015.

RFC7592 OAuth 2.0 Dynamic Client Registration Management Protocol. J. Richer, Ed., M. Jones, J. Bradley, M. Machulak. July 2015.

RFC7636 Proof Key for Code Exchange by OAuth Public Clients. N. Sakimura, Ed., J. Bradley, N. Agarwal. September 2015. (Format: TXT=39482 bytes)

RFC7643 System for Cross-domain Identity Management: Core Schema. P. Hunt,Ed., K. Grizzle, E. Wahlstroem, C. Mortimore. September 2015.

RFC7644 System for Cross-domain Identity Management: Protocol. P. Hunt, Ed.,K. Grizzle, M. Ansari, E. Wahlstroem, C. Mortimore. September 2015.

RFC7662 OAuth 2.0 Token Introspection. J. Richer, Ed. October 2015.

Security Architects Partners' OAuth-Based Identity Standards Glossary

IETF INTERNET DRAFTS AND OTHER SPECIFICATIONS (AS OF DECEMBER 2017)

Internet Draft for OAuth 2.0 Device Flow for Browserless and Input Constrained Devices

TOKEX OAuth 2.0 Token Exchange. See Internet Draft for OAuth 2.0 token exchange, which enables OAuth clients to request and obtain security tokens from authorization servers acting in the role of an Security Token Service (STS, i.e., originally per the WS-Trust specification).

FAPI OpenID Financial API (FAPI) WG

TOKB Internet Draft for using Token Binding with OAuth

OIDC OpenID Connect

PKCE RFC 7636 Proof Key for Code Exchange by OAuth Public Clients

SAML Security Assertion Markup Language

SCIM System for Cross-domain Identity Management (RFC 7643 and RFC 7644)

UMA User Managed Access Protocol, specifications and working group site

EAP Extensible Authentication Protocol (protocol used in wireless networks and point to point connections, defined in RFC 3748and updated by RFC 5247

KuppingerCole Ltd.
Headquarters
Wilhelmstr. 20-22
65185 Wiesbaden | Germany
Tel +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com