Alcatel·Lucent

OAuth Use Cases

Zachary Zeltsan

31 March 2011

Outline

Why use cases?

Present set in the draft draft-zeltsan-oauth-use-cases-01.txt by George Fletcher [gffletch@aol.com], Torsten Lodderstedt [torsten@lodderstedt.net], and Zachary Zeltsan [zachary.zeltsan@alcatel-lucent.com])

- Template for a use case
- Overall list
- Cases supported in OAuth 2.0
- Cases *not* supported in OAuth 2.0

Relations to other organizations

- WAC
- Kantara (UMA)

Proposal

Why use cases?

- The question “what is the use case?” has been mentioned on the list over **100 times** since the beginning of the group.
- We need to understand
  - the high-level view of the function
  - why a certain protocol feature is there (and this is easy to forget!)
  - the relation of the low level detail to the original concept and need
- We need to explain to a broader community *what* we want to achieve

Development of a draft on the use cases was requested (suggested?) by Peter at the OAuth meeting at the IETF 77

Overall list

- Web server
- User-agent
- In-App-Payment (based on Native Application)
- Mobile App
- Device
- Client password credentials
- Assertion
- Content manager
- Access token exchange
- Multiple access tokens
- Gateway for browser-based VoIP applets
- Signed Messages
- Signature with asymmetric secret

Template for a use case:

- Description
- Pre-conditions
- Post-conditions
- Requirements

Cases supported in OAuth 2.0

Authorization code

- Web server

Implicit grant

- User-agent
- Mobile App (as a native application)
- In-App-Payment (Native app. with additional requirements)

Client credentials

- Client password credentials

Extensions

- Assertion

Resource owner password credentials

- Mobile App (as a native application)

Cases *not* supported in OAuth 2.0

- Content manager (requires re-delegation)
- Access token exchange (requires issuance of the multiple access tokens; e.g., one to the client for access to resource server 1, another to the resource server 1 for access to resource server 2)
- Multiple access tokens (requires issuance of the multiple access tokens for access to several resource servers by the client)
- Gateway for browser-based VoIP applets (requires adaptation of OAuth for SIP)
- Signed messages (requires signatures that allow to verify that an access token was issued by an application A to an application B with the owner's authorization)
- Device (requires display of URL of the Authorization Endpoint and Authorization Code in a user-friendly format)
- Signature with asymmetric secret (relies on the use of asymmetric cryptography)

Relations to other organizations

- Wholesale Application Community (WAC)

  The In-App-Payment (based on Native Application) use case has been approved by WAC

- Kantara initiative, User-Managed Access (UMA) use cases

  The use cases have not had a significant consideration

Proposal

- (Try to) adhere to top-down design, preferably driven by use cases
- Maintain the use case list and publish as Informational RFC to accompany each protocol release