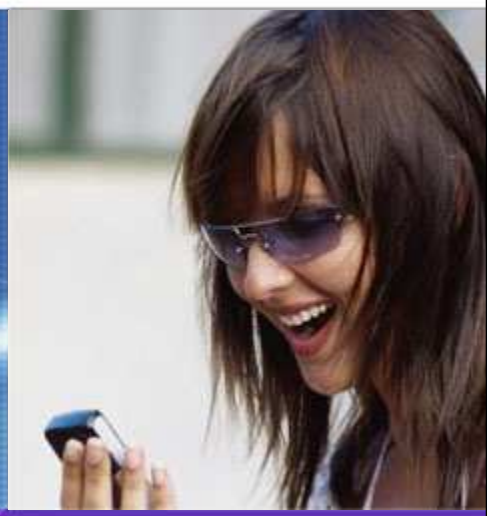
Alcatel·Lucent

OAuth Use Cases



George Fletcher, Torsten Lodderstedt, Zachary Zeltsan

November 2011

Outline

- Why use cases?

  Present set in the draft draft-zeltsan-oauth-use-cases-02 by George Fletcher (gffletch@aol.com), Torsten Lodderstedt (torsten@lodderstedt.net), and Zachary Zeltsan (zachary.zeltsan@alcatel-lucent.com)

- Overall list and supported use cases, template for a use case

- Reviews

  Proposal

  Back-up

  - Cases *not* supported in OAuth 2.0
  - Relations to other organizations
  - Web server (abbreviated example)

Why use cases?

- The questions regarding the use cases is frequently asked:
  - Google's search "use cases" site:http://www.ietf.org/mail-archive/web/oauth/current/ returns more than 60 email messages
- 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 and supported use cases, template for a use case

- Web server *
- User-agent *
- In-App-Payment (based on Native Application)
- Native Application *
- 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

Reviews

Thanks to the reviewers of the version –01

- Melinda Shore (sent to the list http://www.ietf.org/mail-archive/web/oauth/current/msg06161.html)
- Thomas Hardjono (sent to the editors and WG Chairs)

The received comments have been addressed, version –02 was published

Proposal

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

Back-up

Back-up

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

Web server (abbreviated example)

Description:

Alice accesses an application running on a web server at www.printphotos.example.com and instructs it to print her photographs that are stored on a server www.storephotos.example.com. The application at www.printphotos.example.com receives Alice's authorization for accessing her photographs without learning her authentication credentials with www.storephotos.example.com.

Pre-conditions:

- Alice has registered with www.storephotos.example.com to enable authentication

...

Post-conditions:

Procedure results in the application www.printphotos.example.com receiving an authorization code from www.storephotos.example.com ...

Requirements:

- The server www.printphotos.example.com, which hosts an OAuth client, must be capable of issuing the HTTP redirect requests to Alice's user agent - a browser

...