OAuth 2.0 Token Exchange

Mike Jones

July 24, 2014

IETF 90

Background

- Act-As and On-Behalf-Of are supported in WS-Security, WS-Trust
  - Similar to identity impersonation feature in Windows
  - 2 distinct but related concepts
- Both are represented as Security Tokens – JWTs by default
  - Security Tokens same concept as Assertions in draft-ietf-oauth-assertions
  - Support for JWT security tokens required
    - New in draft -01 – can be unsigned when trust model allows
  - Other security token types, such as SAML, also possible

draft-jones-oauth-token-exchange Design Goals

- Act-As
  - Indicates that the requestor wants a token that contains ***claims about two distinct entities***: the requestor and an external entity represented by the token in the `act_as` parameter
- On-Behalf-Of
  - Indicates that the requestor wants a token that contains ***claims only about one entity***: the external entity represented by the token in the `on_behalf_of` parameter

- *Both are special cases of general token exchange functionality – the core function of WS-Trust*

Act-As Scenarios

- Used where composite delegation is required, where the final recipient of the issued token can inspect the entire delegation chain and see not just the client, but all intermediaries
- Enables access control, auditing, and other related activities based on the entire identity delegation chain
- Commonly used in multi-tiered systems to authenticate and pass information about identities between the tiers without having to pass this information at the application/business logic layer

On-Behalf-Of Scenarios

- Used in scenarios where only the identity of the original client is important
- Final recipient can only see claims about the original client
- Information about intermediaries is not preserved
- Commonly used for the proxy pattern, where the client cannot access the Token Service directly but instead communicates through a proxy gateway
- Proxy gateway authenticates the caller and puts information about the caller into the On-Behalf-Of element of the token request that it then sends to the real Token Service for processing
  - Resulting Token contains only claims related to the original client, making the proxy completely transparent to the receiver of the issued token

New Grant Type Used at Token Endpoint

- urn:ietf:params:oauth:grant-type:security-token-request
  - JWT signed by the party requesting the token
  - As of -01, can be unsigned if trust model allows
- Response contains `security_token` element
  - The requested security token
  - Also `security_token_type`

Optional Request Parameters

- `act_as`
  - OPTIONAL request parameter indicates that the requested security token is expected to contain information about the identity represented by the security token that is the value of this parameter, enabling the requesting party to use the returned security token to act as this identity
- `on_behalf_of`
  - OPTIONAL request parameter indicates that the security token is being requested on behalf of another party. The identity of the party upon whose behalf the request is being made is represented by the security token that is the value of this parameter. Proof of eligibility to act on behalf of that identity MAY be conveyed by including an actor Claim identifying the requesting party in the security token

Questions to the Working Group

- Does the working group want to pursue token exchange functionality?
- If so, should we adopt draft-jones-oauth-token-exchange as a starting point?