Extension IDs

https://tools.ietf.org/html/draft-jones-oauth-amr-values-03

This specification establishes a registry for Authentication Method Reference values and defines an initial set of Authentication Method Reference values.

[draft-jones-oauth-mix-up-mitigation-01]

This specification defines an extension to The OAuth 2.0 Authorization Framework that enables the authorization server to dynamically provide the client using it with additional information about the current protocol interaction that can be validated by the client and that enables the client to dynamically provide the authorization server with additional information about the current protocol interaction that can be validated by the authorization server. This additional information can be used by the client and the authorization server to prevent classes of attacks in which the client might otherwise be tricked into using inconsistent sets of metadata from multiple authorization servers, including potentially using a token endpoint that does not belong to the same authorization server as the authorization endpoint used. Recent research publications refer to these as "IdP Mix-Up" and "Malicious Endpoint" attacks.

https://tools.ietf.org/html/draft-denniss-oauth-device-flow-00

The device flow is suitable for OAuth 2.0 clients executing on devices which do not have an easy data-entry method (e.g., game consoles, TVs, picture frames, and media hubs), but where the end-user has separate access to a user-agent on another computer or device (e.g., desktop computer, a laptop, a smart phone, or a tablet).

https://tools.ietf.org/html/draft-bradley-oauth-jwt-encoded-state-05

This draft provides a method for a client to encode one or more elements encoding information about the session into the OAuth 2 "state" parameter.

https://tools.ietf.org/html/draft-bradley-oauth-stateless-client-id-02

This draft provides a method for communicating information about an OAuth client through its client identifier allowing for fully stateless operation.

https://tools.ietf.org/html/draft-jones-oauth-discovery-00

This specification defines a mechanism for an OAuth 2.0 client to discover the resource owner's OAuth 2.0 authorization server and obtain information needed to interact with it, including its OAuth 2.0 endpoint locations and authorization server capabilities.

http://tools.ietf.org/html/draft-ietf-oauth-token-exchange-03

This specification defines a protocol for a lightweight HTTP- and JSON- based Security Token Service (STS) by defining how to request and obtain security tokens from OAuth 2.0 authorization servers, including security tokens employing impersonation and delegation.

https://tools.ietf.org/html/draft-ietf-oauth-signed-http-request-02

This document a method for offering data origin authentication and integrity protection of HTTP requests. To convey the relevant data items in the request a JSON-based encapsulation is used and the JSON Web Signature (JWS) technique is re-used. JWS offers integrity protection using symmetric as well as asymmetric cryptography.

http://tools.ietf.org/html/draft-ietf-oauth-pop-architecture-07

The OAuth 2.0 bearer token specification, as defined in RFC 6750, allows any party in possession of a bearer token (a "bearer") to get access to the associated resources (without demonstrating possession of a cryptographic key). To prevent misuse, bearer tokens must be protected from disclosure in transit and at rest.

Some scenarios demand additional security protection whereby a client needs to demonstrate possession of cryptographic keying material when accessing a protected resource. This document motivates the development of the OAuth 2.0 proof-of-possession security mechanism.

https://datatracker.ietf.org/doc/draft-ietf-ace-oauth-authz/

This memo defines how to use OAuth 2.0 as an authorization framework with Internet of Things (IoT) deployments, thus bringing a well-known and widely used security solution to IoT devices. Where possible vanilla OAuth 2.0 is used, but where the limitations of IoT devices require it, profiles and extensions are provided.