

IETF 121
Dublin
November 2024

Aaron Parecki
Daniel Fett
Joseph Heenan

OAuth Client ID Scheme

**[https://datatracker.ietf.org/doc/draft-parecki-oauth-client-id-scheme/
draft -00](https://datatracker.ietf.org/doc/draft-parecki-oauth-client-id-scheme/draft-00)**

Problem

Root problem is overlap of namespaces

x509_san_uri, redirect_uri, OpenID Federation, Client Metadata Document all use https URLs as the Client ID value

The resulting problems are:

- AS doesn't know how to resolve metadata, and client can't indicate
- Security issues as discovered in OpenID for VP

There are existing deployments that use these https URLs

Client ID Scheme defined by OpenID for Verifiable Presentations

Introduces a namespace for Client IDs

`<client_id_scheme>:<client_id_value>`

- Defines several schemes: `redirect_uri`, `did`, `verifier_attestation`, `x509_san_dns`, `x509_san_uri`
 - e.g. `...&client_id=did:example:1234&...`
scheme value
- Defines the `https` scheme for use by OpenID Federation
 - e.g. `...&client_id=https://example.com/&...`
scheme value
- And fallback for pre-registered clients

Proposal

Define Client ID Scheme as an IETF draft

With fallback for existing ecosystems that use only one scheme

- OpenID Federation
 - https://openid.net/specs/openid-federation-1_0.html
- Client Metadata Documents
 - <https://datatracker.ietf.org/doc/draft-parecki-oauth-client-id-metadata-document/>

Update OpenID for VP and Client Metadata Documents to reference Client ID Scheme draft

Workgroup: Web Authorization Protocol
Internet-Draft: draft-parecki-oauth-client-id-scheme-latest
Published: 6 November 2024
Intended Status: Informational
Expires: 10 May 2025
Authors: A. Parecki D. Fett J. Heenan
 Okta Authlete Authlete



OAuth 2.0 Client ID Scheme

Abstract

This specification defines the concept of a Client Identifier Scheme to enable Authorization Servers and Clients to use more than one mechanism to obtain and validate Client metadata.

<https://datatracker.ietf.org/doc/draft-parecki-oauth-client-id-scheme/>