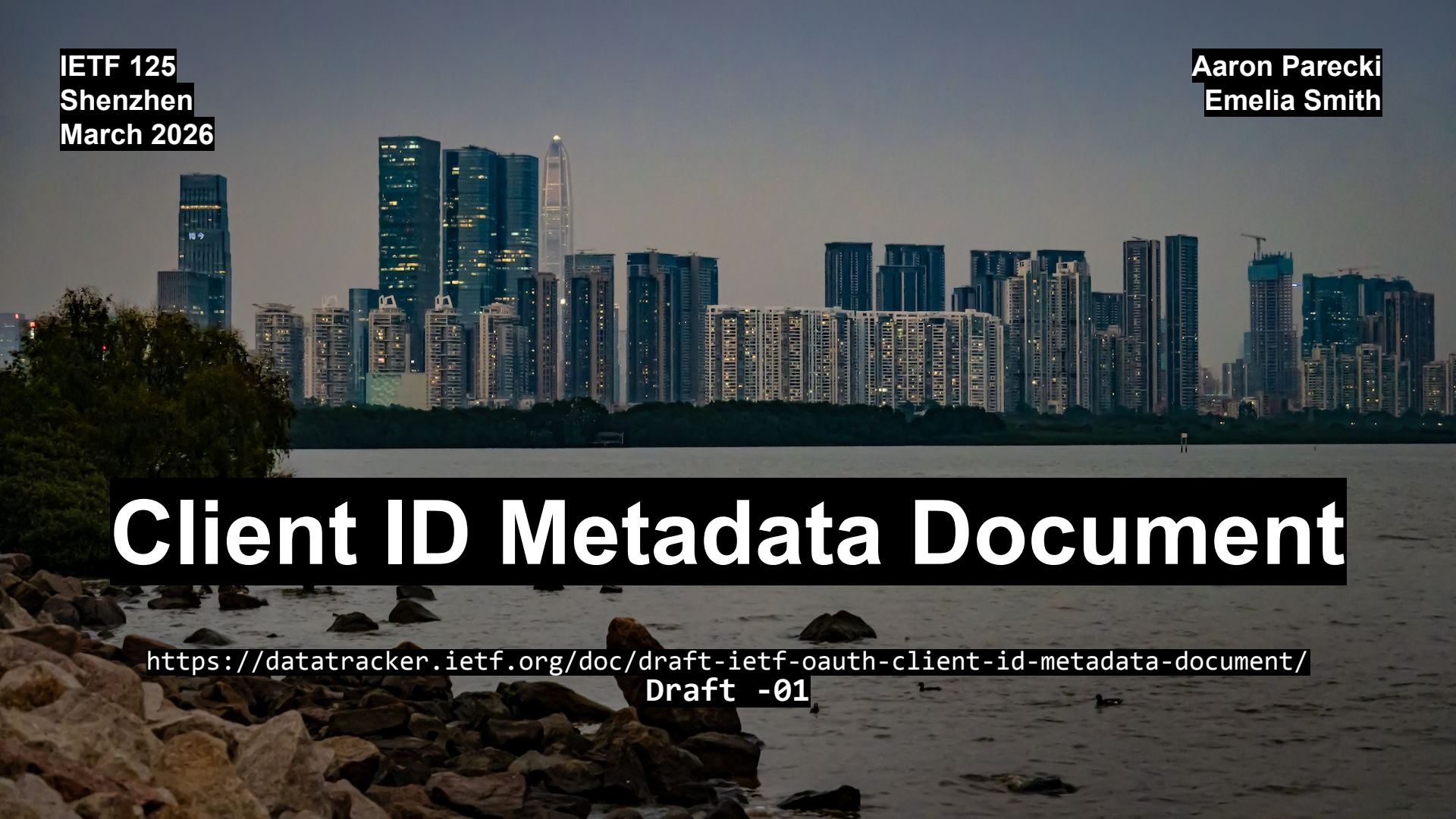


IETF 125
Shenzhen
March 2026

Aaron Parecki
Emelia Smith

Client ID Metadata Document

https://datatracker.ietf.org/doc/draft-ietf-oauth-client-id-metadata-document/

Draft -01

What: Client ID Metadata Document

The client publishes their metadata at a URL (using the Dynamic Client Registration vocabulary)

```
{
  "client_id": "https://example.com/client.json",
  "client_name": "Example Client",
  "client_uri": "https://example.com",
  "logo_uri": "https://example.com/logo.png",
  "redirect_uris": [
    "https://example.com/redirect"
  ]
}
```

The URL is used in an Authorization request

`/authorize?client_id=https://example.com/client.json&...`

https://datatracker.ietf.org/doc/draft-ietf-oauth-client-id-metadata-document/

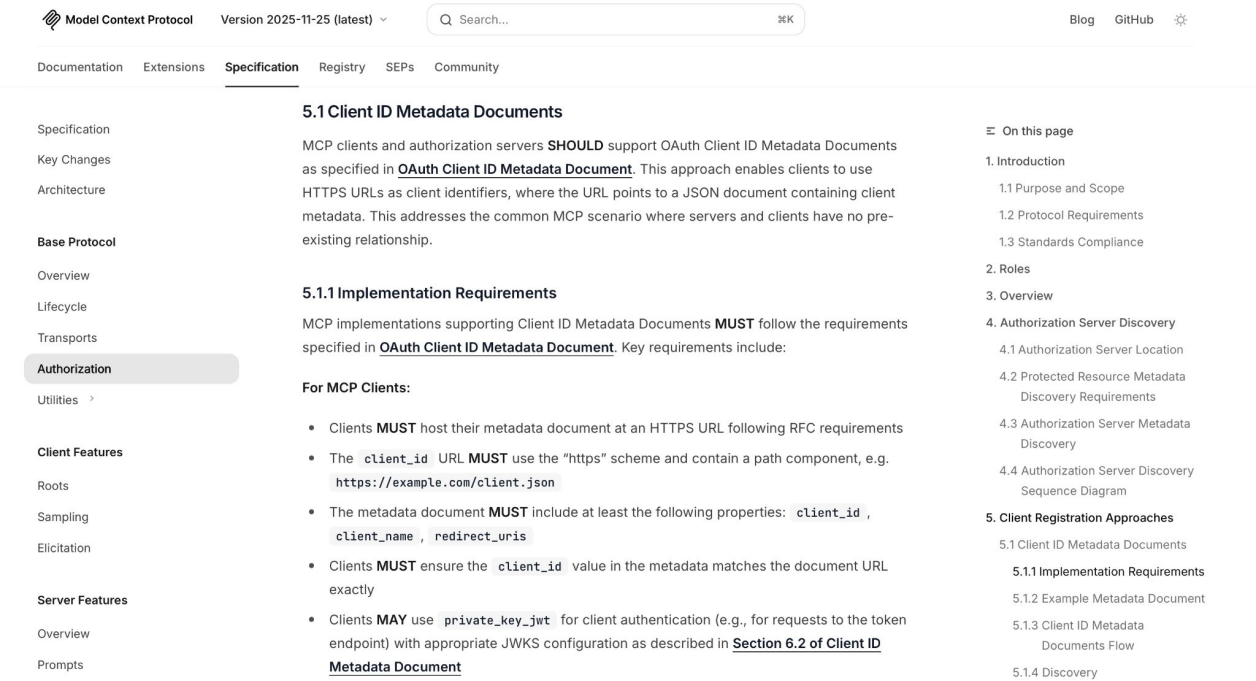
Why?

Pre-registration of clients is not possible when the client developer has no prior relationship with the authorization server, for example:

- Open source chat app connecting to self-hosted chat server
- Apps that connect to self-hosted services, such as Mastodon or WordPress, where there is no single central server to register the OAuth client
- MCP Clients that allow connections to arbitrary MCP servers

What’s new since IETF 124?

MCP (Model Context Protocol) adopted Client ID Metadata Documents as an alternative to Dynamic Client Registration



Launched in the November 25, 2025 MCP spec update

https://modelcontextprotocol.io/specification/2025-11-25/basic/authorization#client-id-metadata-documents

Changes since version -00

Based on feedback given during the call for adoption

- Added guidance for an AS that supports both registered and unregistered clients
- Added additional SSRF security considerations (fetch metadata after authenticating the user, avoid fetching special-use IP ranges)
- Added security consideration for changes in Client Metadata
- Prohibit following redirects (require HTTP 200 response) when fetching metadata document

Open Issues

https://github.com/oauth-wg/draft-ietf-oauth-client-id-metadata-document/issues

Restrictions on URI properties

PR #50 proposes properties like `client_uri`, `logo_uri`, etc MUST be `https` URLs

Avoids potential issues with URIs like `javascript:` or `shortcuts:` if the AS ever renders links or embeds the URLs

But, this prevents optimizations like including a small `data:` URI image

Should this instead just be a security consideration about fetching data from untrusted sources?

Issue #61: jwks vs jwks_uri

Currently there is no guidance/recommendation on including keys in the metadata (`jwks`) vs linking to the keys with `jwks_uri`

Should there be a recommendation/requirement for baseline interoperability, or should this be left to ecosystems to determine interop requirements?

e.g. authorization servers MUST support both, clients can support either

Issue #30: Content-Type Header

Sending an `Accept: application/json` header when fetching enables early rejecting of requests to images, HTML pages, etc

Is `application/json` sufficient, or should this require a more specific content-type such as `application/cimd+json`

Some discussion already on Issue #30 and PR #63

Client Versions

PR #67 adds some text on using `software_version` property

Issue #55 discusses whether to add a formal bidirectional link between different versions of Client ID Metadata Documents

Should we try to define a mechanism to describe client version upgrades?

Further Discussion

https://github.com/oauth-wg/draft-ietf-oauth-client-id-metadata-document/issues