RFC: OpenID with Deferred Token Response?

Frederik Krogsdal Jacobsen, Criipto
IIW 2025

What?

OpenID Connect

…but authorization might take a while

What if authorization is not fast enough to maintain a user agent session?

No:

- Redirects
- Polling while the user waits

Why?

Authorizing specific person “whenever”

Similar to CIBA, but with a frontend and without timeouts

For signatures, we know who we want to authorize

We probably don’t care when exactly the user signs

Validating, Fast and Slow

Identity validation based on machine learning is becoming common

Typical setup:

- Fast machine learning validator
- Certainty too low: slow human validator

“Human-on-the-loop” system

Authorizing AI agent plans

AI Agents with MCP desperately need robust authorization

Plan-and-execute loops can take a while

Use case:

AI agent makes a plan, then asks user for authorization

How?

Everyone does what they want?

Is there enough of a pattern to merit a specification?

Extension of OpenID Connect?

Inspiration:

- OpenID4VCI: Deferred Credential Endpoint
- OpenID CIBA
- RFC 8628: Device Authorization Grant

Poll?

Ping?

Push?

Results from IIW session

- Small extension to OpenID Connect
- Take heavy inspiration from OpenID4VCI: Deferred Credential Endpoint
- Flow modifications:
  - Token endpoint returns a long-lived access token instead of an identity token (MUST use DPoP)
  - Poll/ping design on a new endpoint where access token can be exchanged for an identity token once ready
- Questions:
  - Should client request deferral or should it be a server decision?
  - New endpoint name? (`/deferred_token` would match VCI spec)