The Cambrian Explosion of OAuth and OpenID Specifications

Michael B. Jones and Vladimir Dzhuvinov

OAuth Security Workshop 2025, Reykjavík

The Cambrian Explosion

"an interval of time beginning approximately 538.8 million years ago in the Cambrian period of the early Paleozoic, when a sudden radiation of complex life occurred and practically all major animal phyla started appearing in the fossil record. It lasted for about 13 to 25 million years and resulted in the divergence of most modern metazoan phyla."

– Wikipedia

The Cambrian Explosion of Specifications

“We currently have a Cambrian explosion in Internet and Web standards. Things looked a way simpler and easier to grasp 11 years ago when I had my first experience with the OpenID Connect WG.”

– Vladimir Dzhuvinov, August 2023

“There are too many OAuth specs.” *(paraphrased from memory)*

– Tony Nadalin, July 2016, IETF 96, Berlin

Quantifying the Explosion *(final and near-final specs)*

- 31 OAuth specs
- 13 JOSE & JWT specs
- 13 OpenID Connect specs
- 2 other related IETF specs used by OpenID Connect
- 5 FAPI specs
- 1 MODRNA spec
- 3 eKYC-IDA specs
- 4 SecEvent specs
- 4 Shared Signals specs
- 9 Wallet specs
- 11 COSE specs
- 2 Passwordless Login specs
- 3 Zero-Knowledge Proof specs
- **101 OAuth & OpenID-related specs!**
- And more on the way…
  - 12 active OAuth WG specs, etc.

What’s a developer to do?

- Tony Nadalin tried to stop things
  - Failed to stop PKCE
  - Delayed OAuth Resource Metadata for 8 years (now in RFC Editor queue)
- Companies implementing “carefully curated” sets of specs
  - Implement closely-related specs in libraries, platform offerings
  - With extensibility points enabling the use of more
    - E.g., RAR may not be directly supported, but can be used by applications

Thoughts on stopping things

- People create new specs to scratch their own itches
  - Advocates are often enthusiastic
  - Not easily deterred
- Just because I don’t need something, it doesn’t make them wrong
- Stopping things is hard
  - Takes far more energy to oppose new work than to let it happen

- As a result, new things keep being added
  - Overall, a sign of a healthy body of work

Fear of not stopping things

“If they create a spec to do X, customers will ask me to support it!”

– Anonymous OSW 2025 attendee

“The ever-increasing combinatorial combinations of specs creates a complexity nightmare.”

– Me, during discussions with implementers leading up to OSW

Extensibility paved the road to the explosion

“The authorization server MUST ignore unrecognized request parameters.”

“The client MUST ignore unrecognized response parameters.”

– RFC 6749

“All claims that are not understood by implementations MUST be ignored.”

– RFC 7519

We eagerly sought builders’ perspectives

- I appreciate these conversations Vladimir and I had in preparation
  - Taka Kawasaki and Joseph Heenan of Authlete
  - Brock Allen, Dominick Baier, and Joe DeCock of Duende Software
  - Trevor Thompson and Aaron Parecki of Okta
  - Brian Campbell and David Waite of Ping Identity

Perspectives from these conversations

“We can't build everything.”

“Sometimes we implement things to see if they make sense.”

“It’s hard to know the impact of proposed specs at the time.”

“Saying "no" in standards is wildly useful and little appreciated. It's very hard.”

“Be aware of how new spec proposals interact with existing data models.”

“New specs can cut across and invalidate architectural layering.”

“Implementing even simple new things means fitting into spaghetti.”

“General-purpose RAR implementations don't make sense.”

We’re here to have a conversation with you

- I certainly don’t have all the answers

- ***Your turn!***