

Web Authorization Protocol (oauth)

IETF 90, Toronto

Chairs: Hannes Tschofenig, Derek
Atkins

Responsible AD: Kathleen Moriarty

Mailing List: oauth@ietf.org

Note Well

- **Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:**
 - The IETF plenary session
 - The IESG, or any member thereof on behalf of the IESG
 - Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
 - Any IETF working group or portion thereof
 - Any Birds of a Feather (BOF) session
 - The IAB or any member thereof on behalf of the IAB
 - The RFC Editor or the Internet-Drafts function
- **All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).**
- **Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.**
- **A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.**
- **A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.**

Agenda

- **Welcome & Agenda Bashing** (Chairs, 10min)
- **Dynamic Client Registration** (Justin, 10min)
- **Proof-of-Possession Security** (Hannes, 15min)
- **Token Introspection** (Justin, 15min)
- **OAuth Symmetric Proof of Possession for Code Extension** (Nat, 15min)
- **Providing User Authentication Information to OAuth 2.0 Clients** (Mike, 15min)
- **OAuth 2.0 Token Exchange** (Mike, 15min)
- **Request by JWS ver.1.0 for OAuth 2.0** (Nat, 15min)
- **Summary & Next Steps** (Chairs, 10min)

Milestones

Milestones

- Done Submit 'The OAuth 2.0 Protocol: Bearer Tokens' to the IESG for consideration as a Proposed Standard
- Done Submit 'The OAuth 2.0 Authorization Protocol' to the IESG for consideration as a Proposed Standard
- Done Submit 'An IETF URN Sub-Namespace for OAuth' to the IESG for consideration as a Proposed Standard
- Done Submit 'OAuth 2.0 Threat Model and Security Considerations' to the IESG for consideration as an Informational RFC
- Done Submit 'Token Revocation' to the IESG for consideration as a Proposed Standard
- Done Submit 'OAuth 2.0 Assertion Profile' to the IESG for consideration as a Proposed Standard
[draft-ietf-oauth-assertions](#)
- Done Submit 'SAML 2.0 Bearer Assertion Profiles for OAuth 2.0' to the IESG for consideration as a Proposed Standard
[draft-ietf-oauth-saml2-bearer](#)
- Done Submit 'JSON Web Token (JWT)' to the IESG for consideration as a Proposed Standard
[draft-ietf-oauth-json-web-token](#)
- Done Submit 'JSON Web Token (JWT) Bearer Token Profiles for OAuth 2.0' to the IESG for consideration as a Proposed Standard
[draft-ietf-oauth-jwt-bearer](#)
- Jul 2014 Submit 'OAuth Dynamic Client Registration Protocol' to the IESG for consideration as a Proposed Standard
[draft-ietf-oauth-dyn-reg](#)

+ 1 new milestone currently in Area Director review.

Document Status

Draft	Status	Ballot
draft-ietf-oauth-assertions-17	AD Evaluation (for 9 days) Submitted to IESG for Publication Apr 2013	2 Discusses
draft-ietf-oauth-jwt-bearer-10	AD Evaluation (for 23 days) Submitted to IESG for Publication Aug 2013	-
draft-ietf-oauth-saml2-bearer-21	AD Evaluation (for 6 days) Submitted to IESG for Publication Apr 2013	-
draft-ietf-oauth-json-web-token-25	AD Evaluation (for 23 days) Submitted to IESG for Publication Aug 2013	-

Document Status, cont.

- Use case document removed from the milestone list
 - <http://www.ietf.org/mail-archive/web/oauth/current/msg13113.html>
- Proof-of-Possession Documents approved as WG items
 - <http://www.ietf.org/mail-archive/web/oauth/current/msg13115.html>

Published Security Advisory for "Covert Redirect"

- See <http://oauth.net/advisories/2014-1-covert-redirect/>
- Additional background material:
 - <http://www.thread-safe.com/2014/05/covert-redirect-and-its-real-impact-on.html>
 - <http://nat.sakimura.org/2014/05/08/covert-redirect-is-not-new/>
- Thanks to Pamela Dingle for pushing us to produce a meaningful write-up.