OAuth Working Group
Internet-Draft
Intended status: Standards Track
Expires: 29 October 2026

M. Chen
L. Su
China Mobile

27 April 2026

OAuth 2.0 Agent Authorization Explicit Revocation
draft-chen-oauth-agent-revocation-00

Abstract

The OAuth 2.0 Token Revocation mechanism defined in RFC 7009 enables clients to notify authorization servers that a token is no longer needed. However, that mechanism is limited to single-token operations and does not support batch revocation, cascade propagation, or context-aware semantics at the agent level. With the emergence of autonomous systems and cross-domain agent networks, authorization servers require more granular, traceable revocation semantics.

This document defines an agent-based explicit revocation extension, introducing new endpoints, request/response formats, and coordination protocols to support batch revocation based on agent IDs, cascade propagation, conditional revocation, and verifiable audit trails.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 29 October 2026.

Copyright Notice

Table of Contents

1. Introduction

RFC 7009 defines the standard OAuth 2.0 token revocation flow, which operates at the granularity of individual tokens (access tokens or refresh tokens). This design works well in traditional client-server architectures but reveals significant limitations in emerging scenarios:

Agent Networks: Multiple agent proxies form delegation chains through authorization topology

Autonomous Systems: Agents can dynamically generate sub-agents and distribute permissions

Cross-Domain Collaboration: Agents migrate across different trust domains In these scenarios, revoking access for an upstream agent typically requires simultaneously revoking all its delegated sub-agents. RFC 7009 lacks mechanisms to support such cascade revocation.

Existing RFC 7009 exhibits the following core deficiencies:

Single Granularity: Supports only per-token revocation, cannot batch process by agent ID No Cascade Propagation: After upstream agent revocation, downstream sub-agent tokens remain valid Insufficient

Response Information: 200 OK status does not provide revocation confirmation, execution results, or failure details No Audit Context: Cannot convey revocation reasons, operator identity, or other critical audit information No Event Notification: No standard mechanism to notify relevant parties (e.g., resource servers, downstream agents) of token status changes Missing Conditional Revocation: Does not support suspension, partial permission revocation, or other fine-grained policies

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 RFC2119 [RFC8174].

Readers are expected to be familiar with the terms and concepts described in the core OAuth 2.0 Framework [RFC6749] and [RFC7009].

3. Agent Revocation Endpoint

3.1. Endpoint Definition

To support agent-based explicit revocation, a new endpoint is defined:

```
POST /agent/revoke
```

This endpoint accepts a JSON request body containing the revocation target, reason, and propagation strategy.

3.2. Request Format

The request MUST include the following parameters:

Metadata Field	Type	Required	Description
agent_id	String	Yes	Identifier of the agent to be revoked.
reason	Object	Yes	Revocation reason, containing code and description.
cascade_depth	integer	Yes	Cascade depth, -1 for unlimited, 0 for this agent only.
context	Object	Recommended	Operation context including operator, source_ip, request_id.

Table 1

Status Parameters:

Parameter	Type	Required	Description
revoke_all_tokens	boolean	No	Whether to revoke all tokens for this agent, default true.
revoke_for_duration	integer	No	Temporary suspension duration in seconds, absent means permanent.
revoke_scopes	array	No	List of scopes to be removed.
retain_scopes	array	No	List of scopes to be retained.

Table 2

Example Requst:

```
POST /agent/revoke HTTP/1.1
Host: authorization-server.example.com
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiIs...

{
  "agent_id": "urn:agent:root:12345",
  "reason": {
    "code": "SECURITY_INCIDENT",
    "description": "Agent exhibited anomalous behavior pattern"
  },
  "cascade_depth": -1,
  "context": {
    "operator": "urn:user:admin:security",
    "source_ip": "10.0.0.1",
    "request_id": "req-abc-123"
  },
  "revoke_all_tokens": true
}
```

3.3. Response Format

The server MUST return a JSON response containing execution status and detailed statistics.

Example Successful Response (HTTP 200):

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "status": "completed",
  "transaction_id": "tx-uuid-001",
  "timestamp": "2026-03-25T10:30:00Z",
  "summary": {
    "direct_agents_revoked": 1,
    "cascade_agents_revoked": 3,
    "tokens_revoked": 15,
    "events_emitted": 15,
    "failures": []
  },
  "affected_agents": [
    {"agent_id": "urn:agent:root:12345", "status": "revoked"},
    {"agent_id": "urn:agent:sub:child_1", "status": "revoked"},
    {"agent_id": "urn:agent:sub:child_2", "status": "revoked"},
    {"agent_id": "urn:agent:sub:child_3", "status": "revoked"}
  ],
  "audit_reference": "urn:audit:log:entry-98765"
}
```

Example Failure Response (HTTP 400)

```
HTTP/1.1 400 Bad Request
Content-Type: application/json

{
  "status": "failed",
  "transaction_id": "tx-uuid-002",
  "timestamp": "2026-03-25T10:31:00Z",
  "error": {
    "code": "INVALID_AGENT_ID",
    "description": "The specified agent_id does not exist or has already been revoked."
  },
  "summary": {
    "direct_agents_revoked": 0,
    "cascade_agents_revoked": 0,
    "tokens_revoked": 0,
    "events_emitted": 0,
    "failures": [
      {
        "agent_id": "urn:agent:root:99999",
        "reason": "Agent not found"
      }
    ]
  },
  "audit_reference": "urn:audit:log:entry-98766"
}
```

Response Status Codes

HTTP Status	Description
200 OK	Revocation completed successfully
400 Bad Request	Invalid request parameters (e.g., missing required fields, malformed agent_id)
401 Unauthorized	Missing or invalid authentication credentials
403 Forbidden	Authenticated client lacks permission to revoke the specified agent
404 Not Found	Agent ID not recognized
409 Conflict	Revocation conflicts with an existing operation (e.g., partial revocation already in progress)
429 Too Many Requests	Rate limit exceeded
500 Internal Server Error	Unexpected server error

Table 3

4. Security Considerations

TBD

5. IANA Considerations

TBD

6. Acknowledgements

This document based on RFC7009

7. Informative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC7009] Lodderstedt, T., Ed., Dronia, S., and M. Scurtescu, "OAuth 2.0 Token Revocation", RFC 7009, DOI 10.17487/RFC7009, August 2013, <https://www.rfc-editor.org/rfc/rfc7009>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/rfc/rfc6749>.

Authors' Addresses

Meiling Chen
China Mobile
BeiJing
China
Email: chenmeiling@chinamobile.com

Li Su
China Mobile
BeiJing
China
Email: suli@chinamobile.com