Network Working Group
Internet-Draft
Intended status: Informational
Expires: 21 September 2026

A. Dulaunoy
CIRCL

20 March 2026

The Open Contributions Descriptor
draft-dulaunoy-open-contributions-descriptor-00

Abstract

This document defines the Open Contributions Descriptor (OCD), a JSON format for publishing machine-readable metadata about an organization's participation in the open ecosystem. OCD allows organizations to publish a single discovery document describing open source projects, open data publications, open standards participation, contact information, governance material, and declared relationships to external organizations and projects.

OCD is intended to be published at a predictable well-known location to support automated discovery, indexing, and ecosystem analysis.

Note to Readers

This Internet-Draft is derived from the working specification maintained by the Open Contributions Descriptor project in its public Git repository (https://github.com/ossbase-org/Open-Contributions-Descriptor).

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 21 September 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Introduction

Organizations participate in the open ecosystem in many different ways, including by maintaining software, publishing datasets, contributing to standards, documenting governance, and supporting external communities. Today, this information is usually fragmented across websites, forge hosting platforms, policy pages, and standards organization portals.

The Open Contributions Descriptor (OCD) defines a single JSON [RFC8259] document that aggregates this information in a predictable format. OCD is intended for both human readers and automated tooling. Example use cases include:

* organizational open-source program office inventories;
* cataloging of open data and public APIs;
* ecosystem mapping and stewardship analysis;
* transparency around standards participation; and
* automated discovery of contribution entry points and contact channels.

The design goals of OCD are:

* provide a single discovery endpoint for organizational open activities;
* support both human discovery and machine automation;
* remain extensible without breaking compatibility; and
* allow partial adoption where only some sections are populated.

2. Conventions and Definitions

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] when, and only when, they appear in all capitals, as shown here.

The underlying representation of OCD is JSON as defined by [RFC8259]. Date and date-time values use RFC 3339 formatting [RFC3339].

3. Publication and Discovery

An OCD document is intended to be published at the following location:

https://<organization-domain>/.well-known/open-contributions.json

The use of the /.well-known/ path follows the general mechanism defined in [RFC8615]. Organizations MAY publish the same content at additional locations, but the well-known location is the canonical discovery endpoint.

4. Document Model

An OCD document is a UTF-8 encoded JSON object. Unknown members MAY appear in an OCD document. Consumers MUST ignore members they do not understand, unless a profile or extension explicitly defines stricter processing rules.

The top-level object has the following members.

Field	Type	Requirement	Description
spec_version	string	REQUIRED	Version of the OCD specification implemented by the document.
generated_at	string	REQUIRED	Timestamp indicating when the document was generated.
organization	object	REQUIRED	Metadata describing the publishing organization.
contacts	object	OPTIONAL	Contact information related to open activities.
policies	object	OPTIONAL	Organizational policies relevant to openness and participation.
projects	array	OPTIONAL	Open source projects maintained or contributed to.
open_data	array	OPTIONAL	Published open datasets and feeds.
open_standards	array	OPTIONAL	Participation in standards organizations or specifications.
relationships	array	OPTIONAL	Relationships to external organizations and projects.
extensions	object	OPTIONAL	Organization-specific extensions.

Table 1

4.1. spec_version

The spec_version member identifies the version of the OCD specification used by the document.

4.2. generated_at

The generated_at member MUST be an RFC 3339 date-time string.

4.3. organization

The organization object describes the entity publishing the descriptor.

Field	Type	Requirement	Description
name	string	REQUIRED	Official organization name.
domain	string	REQUIRED	Primary domain hosting the descriptor.
description	string	OPTIONAL	Short description of the organization.
country	string	OPTIONAL	ISO 3166-1 alpha-2 country code.
links	object	OPTIONAL	Public organizational links.

Table 2

4.3.1. organization.links

Field	Description
homepage	Main organizational website.
opensource_page	Dedicated open-source or OSPO page.
github_org	Primary source code organization profile.

Table 3

4.4. contacts

The contacts object provides points of contact relevant to the publishing organization’s open activities.

Field	Type	Description
opensource	object	General open-source contact.
security	object	Security disclosure reference; this SHOULD point to security.txt when applicable.
community	object	Community engagement contact.

Table 4

Each contact object MAY contain the following members.

Field	Type	Description
email	string	Contact email address.
url	string	Contact webpage.

Table 5

4.5. policies

The policies object links to organizational governance and participation policies.

Field	Description
code_of_conduct	Community code of conduct.
contributing	Contribution guidelines.
vulnerability_disclosure	Vulnerability disclosure policy.
license_policy	Licensing strategy or guidance.

Table 6

4.6. projects

The projects member is an array of project objects. Each element describes one open source project.

4.6.1. Project Object

The following project members are defined.

Field	Type	Requirement	Description
name	string	REQUIRED	Project name.
description	string	REQUIRED	Short project description.
repository	object	REQUIRED	Source repository metadata.
links	object	OPTIONAL	Human-facing and machine-facing resources.
participate	object	OPTIONAL	External contribution entry points.
governance	object	OPTIONAL	Governance information.
release	object	OPTIONAL	Release and security lifecycle information.
status	string	OPTIONAL	Project lifecycle state.
tags	array	OPTIONAL	Keywords describing the project.

Table 7

Valid values for status are:

* active: maintained and accepting contributions;
* archived: no active development but preserved; and
* disabled: service or project no longer available.

4.6.2. repository

Field	Requirement	Description
url	REQUIRED	Canonical repository URL.
license	REQUIRED	SPDX license identifier.
type	OPTIONAL	Repository type, for example git.
clone	OPTIONAL	Clone URL.
tests	OPTIONAL	Continuous integration or test URL.

Table 8

4.6.3. links

Field	Description
project_page	Canonical human-readable project page.
homepage	Organization-hosted overview page.
documentation	Official documentation.
demo	Live deployment or demo instance.
releases	Release or download page.
community	Chat, forum, or community hub.
metadata	Machine-consumable descriptors.

Table 9

4.6.4. links.metadata

Field	Description
openapi	URL to an OpenAPI description of the project API.

Table 10

Additional metadata members MAY be added.

4.6.5. participate

Field	Description
issues	Issue tracker URL.
good_first_issues	Beginner-friendly issues.
chat	Real-time communication channel.
docs	Contribution or developer documentation.

Table 11

4.6.6. governance

Field	Description
maintainers	List of maintainer contacts.
codeowners	CODEOWNERS file location.

Table 12

4.6.7. release

Field	Description
changelog	Release history.
security_policy	Project security policy.

Table 13

4.7. open_data

The open_data member is an array of dataset objects.

Field	Type	Requirement	Description
name	string	REQUIRED	Dataset name.
description	string	OPTIONAL	Dataset summary.
license	string	REQUIRED	Data license, for example CC-BY-4.0.
publisher	string	OPTIONAL	Publishing entity.
urls	object	REQUIRED	Access points.
formats	array	OPTIONAL	Available formats.
update_frequency	string	OPTIONAL	Publication cadence.
schema	string	OPTIONAL	Schema definition URL.
tags	array	OPTIONAL	Dataset categories.

Table 14

4.7.1. open_data.urls

Field	Description
landing_page	Human-readable dataset page.
download	Direct dataset download.
api	API endpoint.

Table 15

4.8. open_standards

The open_standards member is an array describing participation in standards bodies.

Field	Type	Description
body	string	Standards organization, for example IETF or W3C.
working_groups	array	Associated working groups.
contributions	array	Contributions made.
contacts	array	Standards participation contacts.

Table 16

4.8.1. contributions

Field	Description
type	Contribution type, such as draft-author, editor, implementation, or review.
title	Contribution title.
url	Reference URL.

Table 17

4.9. relationships

The relationships member allows an organization to declare structured relationships to other organizations and projects. This section supports ecosystem mapping, governance transparency, and machine-readable attribution of stewardship and contribution.

Each relationship object has the following members.

Field	Type	Requirement	Description
type	string	REQUIRED	Relationship type describing the role or interaction.
target	object	REQUIRED	The related organization or project.
since	string	OPTIONAL	RFC 3339 date or date-time when the relationship started.
until	string	OPTIONAL	RFC 3339 date or date-time when the relationship ended.
description	string	OPTIONAL	Human-readable explanation.
evidence	array	OPTIONAL	URLs or structured objects supporting the claim.
contacts	array	OPTIONAL	Contacts for this relationship.
tags	array	OPTIONAL	Keywords for classification and search.
extensions	object	OPTIONAL	Relationship-specific extensions.

Table 18

Recommended values for type are:

* maintains;
* co_maintains;
* supports;
* contributes_to;
* sponsors;
* upstream_of;
* downstream_of;

* member_of; and
* affiliated_with.

4.9.1. target

The target object identifies the related entity.

Field	Type	Requirement	Description
kind	string	REQUIRED	Either organization or project.
name	string	REQUIRED	Display name of the target.
domain	string	OPTIONAL	Domain of the target organization.
ocd	string	OPTIONAL	URL to the target’s OCD document.
url	string	OPTIONAL	Canonical human-readable URL for the target.
project	object	OPTIONAL	Project identifier; required when kind is project.

Table 19

4.9.2. target.project

Field	Type	Requirement	Description
repository_url	string	OPTIONAL	Canonical repository URL.
homepage	string	OPTIONAL	Project homepage or project page URL.
license	string	OPTIONAL	SPDX license identifier.

Table 20

4.9.3. evidence

The evidence member is an array containing either bare URLs or structured objects.

Field	Type	Description
url	string	Evidence URL.
label	string	Short label for humans.
type	string	Evidence type, such as policy, announcement, or repo-metadata.

Table 21

4.10. extensions

The extensions object allows custom additions without breaking compatibility. Consumers MUST ignore unknown extension members. Extension names SHOULD be logically namespaced to reduce collisions.

5. Validation and Processing Rules

An OCD processor:

* MUST parse the document as JSON;
* MUST treat spec_version, generated_at, and organization as required top-level members;
* MUST ignore unknown members;
* SHOULD validate date-time values against RFC 3339;
* SHOULD validate license identifiers against SPDX when such validation is available; and
* SHOULD preserve unrecognized extension content when transforming or proxying an OCD document.

6. Example

The following example illustrates an OCD document.

```
{
  "spec_version": "1.0",
  "generated_at": "2026-02-23T09:00:00Z",
  "organization": {
    "name": "Example Organization",
    "domain": "example.org",
```

```
      "description": "An organization contributing to open source software, open data, a
nd open standards.",
      "country": "LU",
      "links": {
        "homepage": "https://example.org",
        "opensource_page": "https://example.org/open",
        "github_org": "https://github.com/example-org"
      }
    },
    "contacts": {
      "opensource": {
        "email": "opensource@example.org"
      },
      "security": {
        "url": "https://example.org/.well-known/security.txt"
      },
      "community": {
        "email": "community@example.org"
      }
    },
    "policies": {
      "code_of_conduct": "https://example.org/code-of-conduct",
      "contributing": "https://example.org/contributing",
      "vulnerability_disclosure": "https://example.org/security",
      "license_policy": "https://example.org/open/licensing"
    },
    "projects": [
      {
        "name": "Vulnerability Lookup",
        "description": "An open platform to correlate and explore vulnerability intellig
ence.",
        "status": "active",
        "repository": {
          "url": "https://github.com/example-org/vulnerability-lookup",
          "license": "AGPL-3.0",
          "type": "git",
          "clone": "https://github.com/example-org/vulnerability-lookup.git",
          "tests": "https://ci.example.org/job/vulnerability-lookup/"
        },
        "links": {
          "project_page": "https://www.vulnerability-lookup.org",
          "homepage": "https://example.org/projects/vulnerability-lookup",
          "documentation": "https://docs.vulnerability-lookup.org",
          "demo": "https://vulnerability.example.org",
          "releases": "https://github.com/example-org/vulnerability-lookup/releases",
          "community": "https://matrix.to/#/#vulnlookup:matrix.org",
          "metadata": {
            "openapi": "https://vulnerability.example.org/openapi.json"
          }
        },
```

```
        "participate": {
          "issues": "https://github.com/example-org/vulnerability-lookup/issues",
          "good_first_issues": "https://github.com/example-org/vulnerability-lookup/issu
es?q=is%3Aissue+is%3Aopen+label%3A%22good+first+issue%22",
          "chat": "https://matrix.to/#/#vulnlookup:matrix.org",
          "docs": "https://docs.vulnerability-lookup.org"
        },
        "governance": {
          "maintainers": [
            "maintainers@example.org"
          ],
          "codeowners": "https://github.com/example-org/vulnerability-lookup/blob/main/C
ODEOWNERS"
        },
        "release": {
          "changelog": "https://github.com/example-org/vulnerability-lookup/releases",
          "security_policy": "https://github.com/example-org/vulnerability-lookup/securi
ty/policy"
        },
        "tags": [
          "security",
          "vulnerability-management",
          "open-source"
        ]
      }
    ],
    "open_data": [
      {
        "name": "Daily Threat Indicators",
        "description": "Open dataset of curated threat intelligence indicators.",
        "license": "CC-BY-4.0",
        "publisher": "Example Organization",
        "urls": {
          "landing_page": "https://example.org/data/threat-indicators",
          "download": "https://example.org/data/threat-indicators/latest.json",
          "api": "https://example.org/api/threat-indicators"
        },
        "formats": [
          "json",
          "csv"
        ],
        "update_frequency": "daily",
        "schema": "https://example.org/data/threat-indicators/schema.json",
        "tags": [
          "open-data",
          "cybersecurity",
          "threat-intelligence"
        ]
      }
    ],
    "open_standards": [
```

```
      {
        "body": "IETF",
        "working_groups": [
          "openpgp",
          "sidrops"
        ],
        "contributions": [
          {
            "type": "draft-author",
            "title": "Example Secure Exchange Format",
            "url": "https://datatracker.ietf.org/doc/draft-example-secure-exchange/"
          },
          {
            "type": "implementation",
            "title": "Reference implementation",
            "url": "https://github.com/example-org/secure-exchange"
          }
        ],
        "contacts": [
          {
            "email": "standards@example.org"
          }
        ]
      }
    ],
    "relationships": [
      {
        "type": "co_maintains",
        "description": "We co-maintain the upstream project with the foundation and anot
her OSPO.",
        "since": "2023-05-01",
        "target": {
          "kind": "project",
          "name": "Upstream Tooling",
          "url": "https://upstream.example.net/tooling",
          "ocd": "https://upstream.example.net/.well-known/open-contributions.json",
          "project": {
            "repository_url": "https://github.com/upstream/tooling",
            "homepage": "https://upstream.example.net/tooling",
            "license": "MPL-2.0"
          }
        },
        "evidence": [
          "https://github.com/upstream/tooling/blob/main/MAINTAINERS.md",
          "https://github.com/upstream/tooling/graphs/contributors"
        ],
        "contacts": [
          {
            "email": "opensource@example.org"
```

```
          }
        ],
        "tags": [
          "governance",
          "maintenance"
        ]
      }
    ],
    "extensions": {}
  }
```

7. Security Considerations

OCD documents are descriptive metadata and do not directly grant privileges or convey authority. However, consumers might use OCD data to drive discovery, ranking, trust decisions, or automation. A malicious or compromised publisher could therefore provide inaccurate metadata.

Consumers SHOULD treat OCD content as unverified assertions unless backed by independently validated evidence. Consumers that act automatically on OCD content SHOULD apply origin authentication, transport security, and local policy before making trust or security decisions.

Publishing contact information can increase discoverability but can also increase unwanted scraping, profiling, or spam. Publishers SHOULD consider the privacy impact of any personal data included in OCD documents.

8. IANA Considerations

IANA is requested to register the well-known URI suffix open-contributions.json in the "Well-Known URIs" registry established by RFC 8615.

The registry entry should include the following information:

* URI suffix: open-contributions.json
* Change controller: OSSBASE (https://ossbase.org/)
* Specification document(s): This document

This well-known resource is used to discover a JSON document describing an organization’s open contributions profile.

A registration request for this well-known URI suffix has been filed and is tracked at: https://github.com/protocol-registries/well-known-uris/issues/78 (https://github.com/protocol-registries/well-known-uris/issues/78)

9. Normative 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/info/rfc2119>.

[RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002, <https://www.rfc-editor.org/info/rfc3339>.

[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/info/rfc8174>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

[RFC8615] Nottingham, M., "Well-Known Uniform Resource Identifiers (URIs)", RFC 8615, DOI 10.17487/RFC8615, May 2019, <https://www.rfc-editor.org/info/rfc8615>.

Appendix A. References

Author’s Address

Alexandre Dulaunoy
Computer Incident Response Center Luxembourg
122, rue Adolphe Fischer
L-L-1521 Luxembourg
Luxembourg
Phone: +352 247 88444
Email: alexandre.dulaunoy@circl.lu