

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 18 September 2026

G. Lo Presti
CERN
M. B. de Jong
M. Baghbani
Ponder Source
M. Nordin
SUNET
17 March 2026

Open Cloud Mesh
draft-ietf-ocm-open-cloud-mesh-04

Abstract

Open Cloud Mesh (OCM) is a server federation protocol that is used to notify a Receiving Party that they have been granted access to some Resource. It has similarities with authorization flows such as OAuth, as well as with social internet protocols such as ActivityPub and email.

A core use case of OCM is when a user (e.g., Alice on System A) wishes to share a resource (e.g., a file) with another user (e.g., Bob on System B) without transferring the resource itself or requiring Bob to log in to System A.

While this scenario is illustrative, OCM is designed to support a broader range of interactions, including but not limited to file transfers.

Open Cloud Mesh handles interactions only up to the point where the Receiving Party is informed of their access to the Resource. Actual Resource access is subsequently managed by other protocols, such as WebDAV.

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 18 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. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	4
2. Terms	4
2.1. Functions	10
2.1.1. OCM Provider	10
2.1.2. OCM Directory Service	10
2.2. Roles	10
2.2.1. Sending Server	10
2.2.2. Receiving Server	10
3. General Flow	11
4. Establishing Contact	11
4.1. Direct Entry	11
4.2. Public Link Flow	11
4.3. Public Invite Flow	12
4.4. Invite Flow	12
4.4.1. Rationale	12
4.4.2. Steps	12
4.4.3. Invite Acceptance Request Details	13
4.4.4. Invite Acceptance Response Details	14
4.4.5. Addition into address books	15
4.4.6. Invite format	15
4.4.7. Security Advantages	16
5. OCM API Discovery	17
5.1. Introduction	17
5.2. Process	18
5.3. Fields	19

6.	Share Creation Notification	22
6.1.	Fields	22
6.2.	Response	26
6.3.	Decision to Discard	26
6.4.	Receiving Party Notification	27
7.	Share Acceptance Notification	27
7.1.	Fields	28
8.	Resource Access	28
9.	Code Flow	30
9.1.	Token Request	30
9.2.	Token Response	31
9.3.	Error Responses	31
10.	Share Deletion	31
11.	Share Updating	32
12.	Resharing	32
13.	IANA Considerations	32
13.1.	Well-Known URI for the Discovery	32
13.2.	JSContact Types Registry	32
13.3.	JSContact Properties Registry	33
13.4.	JSContact Enum Values Registry	33
14.	Security Considerations	33
14.1.	Trust	33
14.1.1.	httpsig	34
14.2.	Legacy shared secrets	34
14.3.	Code Flow	34
15.	References	34
15.1.	Normative References	34
16.	Appendix A: Multi-factor Authentication	35
17.	Appendix B: JWKS and HTTP Signature Examples	35
17.1.	JWKS Endpoint	36
17.2.	Signing a Request (Sender)	36
17.3.	Verifying a Signature (Receiver)	37
17.4.	Validating the Payload	37
18.	Appendix C: Directory Service	38
19.	Appendix D: Object models	39
19.1.	Address Book	39
19.1.1.	Properties	40
19.1.2.	Relationships	40
19.2.	Contact	40
19.2.1.	Properties	41
19.2.2.	Relationships	41
19.3.	Invite	41
19.3.1.	Properties	42
19.3.2.	Relationships	42
19.4.	Provider	42
19.4.1.	Properties	44
19.5.	Share	44
19.5.1.	Properties	45

19.5.2. Relationships	46
19.6. User	46
19.6.1. Properties	47
19.6.2. Relationships	47
19.7. Resource	48
19.7.1. Properties	48
20. Changes	48
20.1. Version 04	48
20.2. Version 03	49
20.3. Version 02	49
20.4. Version 01	49
21. Acknowledgements	49
Authors' Addresses	50

1. Introduction

Open Cloud Mesh was initially conceived of in 2015 and has been deployed since 2016. OCM has been implemented by several platforms, including CERNBox, Nextcloud, OpenCloud, ownCloud, and Seafile.

The goal of OCM is to provide a secure, scalable, and flexible infrastructure for securely sharing and collaborating on resources and has seen wide adoption, not least in the academic sector.

The core idea of OCM is to make it simple for users to do the right thing. This is achieved by providing a protocol that abstracts away security and authentication details from the users to the servers acting on behalf of the users. Another important point of the protocol is the invitation mechanism that lets users connect over established human relationships and use those connections to establish contact between their respective OCM servers.

2. Terms

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.

We define the following concepts, with some non-normative references to related concepts from OAuth [RFC6749] and elsewhere:

- * ***Resource*** - The piece of data or interaction to which access is being granted, including but not limited to: a file or folder, a video call, a contact, a printer queue, etc.
- * ***Remote Resource*** - A Resource provided by the Sending Server.

- * ***Shared Resource*** - A Resource shared by an OCM Server, becoming a Remote Resource if accepted by the Invite Receiver OCM Server.
- * ***Share*** - A policy rule stating that certain actors have specific access rights to a Resource; it MAY also refer to a record in a database representing this rule.
- * ***Sending Party*** - A person or party who is authorized to create Shares; similar to "Resource Owner" in OAuth [RFC6749], identified by its OCM Address.
- * ***Receiving Party*** - A person, group or party who is granted access to the Resource through the Share; similar to "Requesting Party / RqP" in OAuth-UMA, identified by its OCM Address.
- * ***Share Creation Notification*** - A server-to-server request from the sending server to the receiving server, notifying the receiving server that a Share has been created.
- * ***Sending Server*** - The server that:
 - holds the Resource ("file server" or "Enterprise File Sync and Share (EFSS) server" role),
 - provides access to it (by exposing at least one "API"),
 - takes the decision to create the Share based on user interface gestures from the Sending Party (the "Authorization Server" role in OAuth [RFC6749]),
 - takes the decision about authorizing attempts to access the Resource (the "Resource Server" role in OAuth [RFC6749]),
 - sends out Share Creation Notifications when appropriate (see below).
- * ***Receiving Server*** - The server that:
 - receives Share Creation Notifications (see below),
 - actively or passively notifies the receiving user or group of any incoming Share Creation Notification,
 - acts as an API client, allowing the receiving user to access the Resource through an API (e.g., WebDAV [RFC4918]) of the sending server.

- * ***Sending Gesture*** - A user interface interaction from the Sending Party to the Sending Server, conveying the intention to create a Share.
- * ***Share Creation*** - The addition of a Share to the database state of the Sending Server, in response to a successful Sending Gesture or for another reason.
- * ***Sharing User*** - A user providing access to a Resource through a Share.
- * ***FQDN*** - Fully Qualified Domain Name, such as "cloud.example.org".
- * ***OCM Server*** - A server that supports OCM.
- * ***OCM API Discovery*** - Process of evaluating properties of a Remote Resource, after establishing contact with an OCM Server.
- * ***Discovering Server*** - A server that tries to obtain information in OCM API Discovery.
- * ***Discoverable Server*** - A server that tries to supply information in OCM API Discovery.
- * ***Federation*** - A group of OCM Providers that have established mutual trust and agree on certain policies for interaction. A Federation MAY be facilitated by a Directory Service.
- * ***FQDN*** - Fully Qualified Domain Name, such as "cloud.example.com".
- * ***Invite Acceptance Gesture*** - Gesture from the Invite Receiver to the Invite Receiver OCM Server, supplying the Invite Token as well as the OCM Address of the Invite Sender, effectively allowlisting the Invite Sender OCM Server for sending Share Creation Notifications to the Invite Receiver OCM Server.
- * ***Invite Acceptance Response*** - HTTP response to the Invite Acceptance Request.
- * ***Invite Acceptance Request*** - API call from the Invite Receiver OCM Server to the Invite Sender OCM Server, supplying the Invite Token as well as the OCM Address of the Invite Receiver, effectively allowlisting the Invite Sender OCM Server for sending Share Creation Notifications to the Invite Receiver OCM Server.
- * ***Invite Creation Gesture*** - Gesture from the Invite Sender to the Invite Sender OCM Server, resulting in the creation of an Invite Token.

- * ***Invite Message*** - Out-of-band message used to establish contact between parties and servers in the Invite Flow, containing an Invite Token (see below) and the Invite Sender's OCM Address.
- * ***Invite Receiver*** - The party receiving an Invite, identified by its OCM Address.
- * ***Invite Receiver OCM Server*** - The server holding an address book used by the Invite Receiver, to which details of the Invite Sender are to be added.
- * ***Invite Sender*** - The party sending an Invite, identified by its OCM Address.
- * ***Invite Sender OCM Server*** - The server holding an address book used by the Invite Sender, to which details of the Invite Receiver are to be added.
- * ***Invite String*** - A base64 encoded string containing an Invite Token and the FQDN of an Invite Sender OCM Server joined by an @-sign.
- * ***Invite Token*** - A hard-to-guess string used in the Invite Flow, generated by the Invite Sender OCM Server and linked uniquely to the Invite Sender's OCM Address.
- * ***OCM Address*** - identifies a user or group "at" an OCM Server. The OCM Address contains a server specific Party identifier, a host locating the OCM Server and an optional port. The OCM Address is not a URI as it does not have scheme and the identifier may contain reserved characters.

ocm-address = identifier "@" host [":" port]

The identifier is an opaque, case-sensitive UTF-8 string. It is separated from the host by the last "@" in the OCM Address. It is possible to have multiple @-signs in a OCM-address, e.g. when an email address is the local part of the address like nomen.nescio@example.org@ocm.example.org.

host is an IP literal encapsulated within square brackets, an IPv4 address in dotted decimal form, or a registered name as described in [RFC3986].

host = IP-literal / IPv4address / reg-name

The optional port subcomponent can be used to specify a port to use for discovery (see Discovery Process).

The OCM Server MUST be discoverable at the given host and optional port via the Well-Known [RFC8615] path /.well-known/ocm. The OCM Address MUST NOT contain a path.

- * ***OCM API Discovery*** - Process of evaluating properties of a Remote Resource, after establishing contact with an OCM Server.
- * ***OCM Server*** - A server that has the OCM Provider function.
- * ***Discovering Server*** - A server that tries to obtain information in OCM API Discovery.
- * ***OCM Notification*** - A message from the Receiving Server to the Sending Server or vice versa, using the OCM Notifications endpoint.
- * ***Receiving Party*** - A person, group or party who is granted access to the Resource through the Share; similar to "Requesting Party / RqP" in OAuth-UMA, identified by its OCM Address.
- * ***Receiving Server*** - The server that:
 - receives Share Creation Notifications (see below),
 - actively or passively notifies the receiving user or group of any incoming Share Creation Notification,
 - acts as an API client, allowing the receiving user to access the Resource through an API (e.g., WebDAV [RFC4918]) of the sending server.
- * ***Remote Resource*** - A Resource provided by the Sending Server.
- * ***Resource*** - The piece of data or interaction to which access is being granted, including but not limited to: a file or folder, a video call, a contact, a printer queue, etc.
- * ***Sending Gesture*** - A user interface interaction from the Sending Party to the Sending Server, conveying the intention to create a Share.
- * ***Sending Party*** - A person or party who is authorized to create Shares; similar to "Resource Owner" in OAuth [RFC6749], identified by its OCM Address.
- * ***Sending Server*** - The server that:
 - holds the Resource for instance, a file server,

- provides access to it (by exposing at least one "API"),
 - takes the decision to create the Share based on user interface gestures from the Sending Party (the "Authorization Server" role in OAuth [RFC6749]),
 - takes the decision about authorizing attempts to access the Resource (the "Resource Server" role in OAuth [RFC6749]),
 - sends out Share Creation Notifications when appropriate (see below).
- * ***Share*** - A policy rule stating that certain actors have specific access rights to a Resource; it MAY also refer to a record in a database representing this rule.
 - * ***Share Creation*** - The addition of a Share to the database state of the Sending Server, in response to a successful Sending Gesture or for another reason.
 - * ***Share Creation Notification*** - A server-to-server request from the sending server to the receiving server, notifying the receiving server that a Share has been created.
 - * ***Share Name*** - A human-readable string, provided by the Sending Party or the Sending Server, to help the Receiving Party understand which Resource the Share grants access to.
 - * ***Share Permissions*** - protocol-specific allowances granted to the Receiving Party on the modes of accessing the Resource.
 - * ***Share Requirements*** - Protocol-specific restrictions on the modes of accessing the Resource.
 - * ***Shared Resource*** - A Resource shared by an OCM Server, becoming a Remote Resource if accepted by the Invite Receiver OCM Server.
 - * ***Sharing User*** - A user providing access to a Resource through a Share.
 - * ***Trusted Server*** - An OCM Server that is considered trustworthy by another OCM Server, based on out-of-band information, federation membership or prior interactions, SHOULD be recorded in an internal registry of trusted servers, that SHOULD be updated over time based on new information. The registry SHOULD include the FQDN of the trusted server and the Public Key used for HTTP Signatures. It MAY also include additional metadata such as the inviteAcceptDialog URL or supported capabilities.

- * ***WAYF Page*** - A Where-Are-You-From page is a discovery service used to identify the OCM Server of an Invite Receiver.

2.1. Functions

Open Cloud Mesh defines distinct functions. It is not necessary for an implementation to provide all of them. In fact, it may be useful to have separate implementations for different functions.

2.1.1. OCM Provider

An OCM Provider is an entity that can take on the two `_roles_` of a `_Sending Server_` and a `_Receiving Server_`. An OCM Provider **MUST** be a `_Discoverable Server_` and **SHOULD** be able to receive `_Notifications_`.

2.1.2. OCM Directory Service

An OCM Directory Service is an entity that exposes information about a `_Federation_` of OCM Providers.

2.2. Roles

Open Cloud Mesh defines two distinct roles that an OCM Provider **MUST** take on: the `_Sending Server_` role and the `_Receiving Server_` role.

2.2.1. Sending Server

A Sending Server is an OCM Provider that holds Resources and exposes APIs to allow access to them. It allows its users to create `_Shares_` to give other users access to those Resources. A Sending Server **MAY** provide its users with the ability to generate `_Invites_` to establish contact with other users on other OCM Providers. When doing so it **MAY** provide a `_WAYF Page_` to facilitate the Invite Flow. The WAYF page **MAY** be limited to a set of trusted OCM Providers, for instance those in the same `_Federation_`.

2.2.2. Receiving Server

A Receiving Server is an OCM Provider that receives `_Share_ Creation Notifications` from Sending Servers, notifies its users about incoming `_Shares_`, and acts as an API client to allow its users to access Remote Resources. It **MAY** provide its users with an `_Address Book_` of `_Contacts_` and the ability to accept `_Invites_`.

In Appendix D, an object model is presented as a non-normative guide for implementers to understand the relationships between these terms.

3. General Flow

The lifecycle of an Open Cloud Mesh Share starts with prerequisites such as establishing trust, establishing contact, and OCM API Discovery.

Then the share creation involves the Sending Party making a Sending Gesture to the Sending Server, the Sending Server carrying out the actual Share Creation, and the Sending Server sending a Share Creation Notification to the Receiving Server.

After this, the Receiving Server MAY notify the Receiving Party and/or the Sending Server, and will act as an API client through which the Receiving Party can access the Resource. The Receiving Party or the Sending Party MAY then update or delete the Share: the respective Server MAY send a Notification to the other party about the change.

4. Establishing Contact

Before the Sending Server can send a Share Creation Notification to the Receiving Server, it MUST establish the Receiving Party's OCM Address (containing the Receiving Server's FQDN, and the Receiving Party's identifier), among other things. Some steps may precede the Sending Gesture, allowing the Sending Party to establish (with some level of trust) the OCM Address of the Receiving Party. In other cases, establishing the OCM Address of the Receiving Party happens as part of the Sending Gesture.

4.1. Direct Entry

The simplest way for this is if the Receiving Party shares their OCM Address with the Sending Party through some out-of-band means, and the Sending Party enters this string into the user interface of the Sending Server, by means of typing or pasting into an HTML form, or clicking a link to a URL that includes the string in some form.

4.2. Public Link Flow

An interface for anonymously viewing a Resource on the Sending Server MAY allow any internet user to type or paste an OCM address into an HTML form, as a Sending Gesture. This means that the Sending Party and the Receiving Party could be the same person, so contact between them does not need to be explicitly established.

4.3. Public Invite Flow

Similarly, an interface on the Sending Server MAY allow any internet user to type or paste an OCM address into an HTML form, as a Sending Gesture for a given Resource, without itself providing a way to access that particular Resource. A link to this interface could then for instance be shared on a mailing list, allowing all subscribers to effectively request access to the Resource by making a Sending Gesture to the Sending Server with their own OCM Address.

4.4. Invite Flow

4.4.1. Rationale

Many methods for establishing contact allow unsolicited contact with the prospective Receiving Party whenever that party's OCM Address is known. The Invite Flow requires the Receiving Party to explicitly accept it before it can be used, which establishes bidirectional trust between the two parties involved.

OCM Servers MAY enforce a policy to only accept Shares between such trusted contacts, or MAY display a warning to the Receiving Party when a Share Creation Notification from an unknown Sending Party is received

4.4.2. Steps

- * the Invite Sender OCM Server generates a unique Invite Token and helps the Invite Sender to create the Invite Message
- * the Invite Sender uses some out-of-band communication to send the Invite Message, containing the Invite Token and the Invite Sender OCM Server FQDN, to the Invite Receiver
- * the Invite Receiver navigates to the Invite Receiver OCM Server and makes the Invite Acceptance Gesture. This step MAY be facilitated if the Invite Sender OCM Server implements a WAYF Page, such that the Invite Message would include a link to it for the Invite Receiver to navigate to: the Invite Receiver would then be able to indicate their OCM Server and proceed with the Invite Acceptance Gesture without manually copying the Invite Token.
- * the Invite Receiver OCM Server discovers the OCM API of the Invite Sender OCM Server using generic OCM API Discovery (see section below)
- * the Invite Receiver OCM Server sends the Invite Acceptance Request to the Invite Sender OCM Server

4.4.3. Invite Acceptance Request Details

Whereas the precise syntax of the Invite Message and the Invite Acceptance Gesture will differ between implementations, the Invite Acceptance Request SHOULD be a HTTP POST request:

- * to the /invite-accepted path in the Invite Sender OCM Server's OCM API
- * using application/json as the Content-Type HTTP request header
- * its request body containing a JSON document representing an object with the following string fields:
 - REQUIRED: recipientProvider - FQDN of the Invite Receiver OCM Server.
 - REQUIRED: token - The Invite Token. The Invite Sender OCM Server SHOULD recall which Invite Sender OCM Address this token was linked to.
 - REQUIRED: userID - The Invite Receiver's identifier at their OCM Server.
 - REQUIRED: email - Non-normative / informational; an email address for the Invite Receiver. Not necessarily at the same FQDN as their OCM Server.
 - REQUIRED: name - Human-readable name of the Invite Receiver, as a suggestion for display in the Invite Sender's address book
- * using TLS
- * using httpsig [RFC9421]

The Invite Receiver OCM Server SHOULD apply its own policies for trusting the Invite Sender OCM Server before making the Invite Acceptance Request.

Since the Invite Flow does not require either Party to type or remember the userID, this string does not need to be human-memorable. Even if the Invite Receiver has a memorable username at the Invite Receiver OCM Server, this userID that forms part of their OCM Address does not need to match it.

Also, a different userID could be given out to each contact, to avoid correlation of identities.

If the Invite Sender OCM Server implements a WAYF Page, such a page MAY include a fixed list of servers, in addition to, or instead of, a free-text input where any OCM Server can be entered. This is especially useful if the Invite Sender is part of a federation of associated OCM Servers. In order to populate the list of associated OCM Servers, the Invite Sender's server MAY make use of a Directory Service, which is expected to follow the specification detailed in Appendix C.

Implementors that provide a WAYF Page SHOULD make the URL for the API endpoint of such a Directory Service configurable, allowing the OCM Server to be part of a network of associated OCM Servers. The configuration mechanism MAY allow an OCM Server to be part of multiple networks, thus displaying a union of multiple lists in its WAYF Page.

4.4.4. Invite Acceptance Response Details

The Invite Acceptance Response SHOULD be a HTTP response:

- * in response to the Invite Acceptance Request
- * using application/json as the Content-Type HTTP response header
- * its response body containing a JSON document representing an object with the following string fields:
 - REQUIRED: userID - the Invite Sender's identifier at their OCM Server
 - REQUIRED: email - non-normative / informational; an email address for the Invite Sender. Not necessarily at the same FQDN as their OCM Server
 - REQUIRED: name - human-readable name of the Invite Sender, as a suggestion for display in the Invite Receiver's address book

A 200 response status means the Invite Acceptance Request was successful. A 400 response status means the Invite Token is invalid or does not exist. A 403 response status means the Invite Receiver OCM Server is not trusted to accept this Invite. A 409 response status means the Invite was already accepted.

The Invite Sender OCM Server SHOULD verify the HTTP Signature on the Invite Acceptance Request and apply its own policies for trusting the Invite Receiver OCM Server before processing the Invite Acceptance Request and sending the Invite Acceptance Response.

As with the userID in the Invite Acceptance Request, the one in the Response also doesn't need to be human-memorable, doesn't need to match the Invite Sender's username at their OCM Server.

4.4.5. Addition into address books

Following these step, both servers MAY display the name of the other party as a trusted or allowlisted contact, and enable selecting them as a Receiving Party. OCM Servers MAY enforce a policy to only accept Share Creation Notifications from such trusted contacts, or MAY display a warning to users when a Share Creation Notification from an unknown party is received.

Both servers MAY also allowlist each other as a server with which at least one of their users wishes to interact.

In addition, if the identity provider of either server supports the registration of external users, it may happen that the just received email contact from the other party matches an external user already known in the local identity provider, and therefore already present in the address book. In such a case, implementers MAY support linking of the two identities belonging to that same user, so that when a Share Creation gesture is made to that recipient, both a regular share and an OCM Share Creation Notification are issued.

Note that Invites act symmetrically, so once contact has been established, both the Invite Sender and the Invite Receiver MAY take on either the Sending Party or the Receiving Party role in subsequent Share Creation events.

Both parties MAY delete the other party from their address book at any time without notifying them.

4.4.6. Invite format

To accept an invite, two pieces of information are required: a token and a provider. There are two recognized formats:

- * *Invite string format:* A base64-encoded string containing the token and the provider's FQDN, joined by an @ sign. Example:

If the token is a55a966e-15c1-4cb9-a39d-4e4c54399baf and the provider is cloud.example.org, the combined string is a55a966e-15c1-4cb9-a39d-4e4c54399baf@cloud.example.org, which when base64-encoded becomes
YTU1YTk2NmUtMTVjMS00Y2I5LWEzOWQtNGU0YzU0Mzk5YmFmQG15LWNsb3VkLXN0b3JhZ2Uub3Jn.

When parsing an invite string, implementors must base64-decode it, then split on the last @ sign, taking care to allow multiple @ characters in the token part.

- * ***Link format:** If the inviting OCM Server supports a WAYF page, the invite may be provided as a link with the token as a request parameter. Example:

```
https://cloud.example.org/wayf?token= a55a966e-15c1-4cb9-a39d-4e4c54399baf
```

Implementations MUST be able to accept invites in the invite string format. This format is considered canonical. The link format is only useful if the Receiving OCM Server exposes the `inviteAcceptDialog` in its Discovery endpoint. Implementations SHOULD support the link format when they implement a WAYF Page that leverages those `inviteAcceptDialog` targets.

4.4.7. Security Advantages

It is important to underscore the value of the Invite in this scenario, as it provides four important security advantages. First of all, if the Receiving Server blocks Share Creation Notifications from Sending Parties who are not in the address book of the Receiving Party, then this protects the Receiving Party from receiving unsolicited Shares. An attacker could still send the Receiving Party an unsolicited Share, but they would first need to convince the Receiving Party through an out-of-band communication channel to accept their invite. In many use cases, the Receiving Party has had other forms of contact with the Sending Party (e.g., in-person or email back-and-forth). The out-of-band Invite Message thus leverages the filters and context which the Receiving Party may already benefit from in that out-of-band communication. For instance, a careful Receiving Party MAY choose to only accept Invites that reach them via a private or moderated messaging platform.

Second, when the Receiving Party accepts the Invite, the Receiving Server knows that the Sending Server they are about to interact with is trusted by the Sending Party, which in turn is trusted by the Receiving Party, which in turn is trusted by them. In other words, one of their users is requesting the allowlisting of a server they wish to interact with, in order to interact with a party they know out-of-band. This gives the Receiving Server reason to put more trust in the Sending Server than it would put into an arbitrary internet-hosted server.

Third, equivalently, the Sending Server knows it is essentially registering the Receiving Server as an API client at the request of the Receiving Party, to whom the right to request this has been traceably delegated by the Sending Party, which is one of its registered users.

Fourth, related to the second one, it removes the partial 'open relay' problem that exists when the Sending Server is allowed to include any Receiving Server FQDN in the Sending Gesture. Without the use of Invites, a Distributed Denial of Service attack could be organised if many internet users collude to flood a given OCM Server with Share Creation Notifications which will be hard to distinguish from legitimate requests without human interaction. An unsolicited (invalid) Invite Acceptance Request is much easier to filter out than an unsolicited (possibly valid, possibly invalid) Share Creation Notification Request, since the Invite Acceptance Request needs to contain an Invite Token that was previously uniquely generated at the Invite Sender OCM server.

5. OCM API Discovery

5.1. Introduction

After establishing contact as discussed in the previous section, the Sharing User MAY send the Share Creation Gesture to the Sending Server. The Sharing User MUST provide the following information:

- * Resource to be shared
- * Protocol to be offered for access
- * Sending Party's identifier
- * Receiving Party's identifier
- * Receiving Server FQDN
- * OPTIONAL: Share Requirements
- * OPTIONAL: Share Name
- * OPTIONAL: Share Permissions

The next step is for the Sending Server to additionally discover:

- * if the Receiving Server is trusted
- * if the Receiving Server supports OCM

- * if so, which version and with which optional functionality
- * at which URL
- * the public key the Receiving Server will use for HTTP Signatures (if any)

The Sending Server MAY first perform denylist and allowlist checks on the FQDN.

If a finite allowlist of Receiving Servers exists on the Sending Server side, then this list MAY already contain all necessary information.

If the FQDN passes the denylist and/or allowlist checks, but no details about its OCM API are known, the Sending Server can use the following process to try to fetch this information from the Receiving Server.

This process MAY be influenced by a VPN connection and/or IP allowlisting.

When OCM API Discovery can occur in preparation of a Share Creation Notification, the Sending Server takes on the 'Discovering Server' role and the Receiving Server plays the role of 'Discoverable Server'.

5.2. Process

At the start of the process, the Discovering Server has either an OCM Address, or just an FQDN from for instance the recipientProvider field of an Invite Acceptance Request.

Step 1: In case it has an OCM Address, it SHOULD first extract <fqdn> from it (the part after the last @ sign). Step 2: The Discovering Server SHOULD attempt OCM API Discovery via a HTTP GET request to https://<fqdn>/.well-known/ocm. Step 3: If that results in a valid HTTP response with a valid JSON response body within reasonable time, go to step 7. Step 4: If not, try a HTTP GET with https://<fqdn>/ocm-provider as the URL instead. Step 5: If that results in a valid HTTP response with a valid JSON response body within reasonable time, go to step 7. Step 6: If not, fail. Implementations MAY fallback to HTTP instead of HTTPS in testing setups and retry steps 2-5, in particular when an optional port is given in the address. Step 7: The JSON response body is the data that was discovered.

5.3. Fields

The JSON response body offered by the Discoverable Server SHOULD contain the following information about its OCM API:

- * REQUIRED: enabled (boolean) - Whether the OCM service is enabled at this endpoint
- * REQUIRED: apiVersion (string) - The OCM API version this endpoint supports. Example: "1.3.0"
- * REQUIRED: endPoint (string) - The URI of the OCM API available at this endpoint. Example: "https://cloud.example.org/ocm"
- * OPTIONAL: provider (string) - A friendly branding name of this endpoint. Example: "MyCloudStorage"
- * REQUIRED: resourceTypes (array) - A list of all resource types this server supports in both the Sending Server role and the Receiving Server role, with their access protocols. Each item in this list MUST itself be an object containing the following fields:
 - name (string) - A supported resource type (file, calendar, contact, ...). Implementations MUST offer support for at least one resource type, where file is the commonly supported one. Each resource type is identified by its name: the list MUST NOT contain more than one resource type object per given name.
 - shareTypes (array of string) - The supported recipient share types. MUST contain "user" at a minimum, plus optionally "group" and "federation". Example: ["user"]
 - protocols (object) - The supported protocols for accessing Shared Resources of this type. Implementations that offer file Resources MUST support at least webdav, any other combination of Resources and protocols is optional. Example:

```
{
  "webdav": "/remote/dav/ocm/",
  "webapp": "/app/ocm/",
  "talk": "/apps/spread/api/"
}
```

Fields: - webdav (string) - The top-level WebDAV [RFC4918] path at this endpoint. In order to access a Remote Resource, implementations SHOULD use this path as a prefix (see sharing examples). - webapp (string) - The top-level path for web apps

at this endpoint. In order to access a remote web app, implementations SHOULD use this path as a prefix (see sharing examples). - ssh (string) - The top-level address in the form host:port of an endpoint that supports ssh and scp with a public/private key based authentication. - Any additional protocol supported for this Resource type MAY be advertised here, where the value MAY correspond to a top-level URI to be used for that protocol.

- * OPTIONAL: capabilities (array of string) - The optional capabilities supported by this OCM Server. As implementations MUST accept Share Creation Notifications to be compliant, it is not necessary to expose that as a capability. Example: ["exchange-token", "webdav-uri"]. The array MAY include one or more of the following items:
 - "enforce-mfa" - to indicate that this OCM Server can apply a Sending Server's MFA requirements for a Share on their behalf.
 - "exchange-token" - to indicate that this OCM Server exposes a [RFC6749]-compliant endpoint, which allows to exchange a secret received in the protocol properties of a Share Creation Notification for a short-lived bearer token.
 - "http-sig" - to indicate that this OCM Server supports [RFC9421] HTTP Message Signatures and advertises public keys in the format specified by [RFC7517] at the /.well-known/jwks.json endpoint for signature verification.
 - "invites" - to indicate the server would support acting as an Invite Sender or Invite Receiver OCM Server. This might be useful for suggesting to a user that existing contacts might be upgraded to the more secure (and possibly required) invite flow.
 - "notifications" - to indicate that this OCM Server handles notifications to exchange updates on shares and invites.
 - "invite-wayf" - to indicate that this OCM Server exposes a WAYF Page to facilitate the Invite flow.
 - "webdav-uri" - to indicate that this OCM Server can append a relative URI to the path listed for WebDAV [RFC4918] in the appropriate resourceTypes entry

- "protocol-object" - to indicate that this OCM Server can receive a Share Creation Notification whose protocol object contains one property per supported protocol instead of containing the standard name and options properties.
- * OPTIONAL: criteria (array of string) - The criteria for accepting a Share Creation Notification. As all Receiving Servers SHOULD require the use of TLS in API calls, it is not necessary to expose that as a criterium. Example: ["http-request-signatures"]. The array MAY include for instance:
 - "http-request-signatures" - to indicate that API requests without http signatures will be rejected.
 - "token-exchange" - to indicate that API requests without token exchange will be rejected (see the Code Flow (Section 9) section).
 - "denylist" - some servers MAY be blocked based on their IP address
 - "allowlist" - unknown servers MAY be blocked based on their IP address
 - "invite" - an invite MUST have been exchanged between the sender and the receiver before a Share Creation Notification can be sent
- * DEPRECATED: publicKey (object) - Use public keys at /.well-known/jwks.json instead for RFC 9421 support.
- * OPTIONAL: inviteAcceptDialog (string) - URL path of a web page where a user can accept an invite, when query parameters "token" and "providerDomain" are provided. Implementations that offer the "invites" capability SHOULD provide this URL as well in order to enhance the UX of the Invite Flow. If for example "/index.php/apps/sciencemesh/accept" is specified here then a WAYF Page SHOULD redirect the end-user to /index.php/apps/sciencemesh/accept?token=zi5kooKu3ivohr9a&providerDomain=cloud.example.org.
- * OPTIONAL: tokenEndPoint (string) - URL of the token endpoint where the Sending Server can exchange a secret for a short-lived bearer token. Implementations that offer the "exchange-token" capability MUST provide this URL as well. Example:
"https://cloud.example.org/ocm/token".

6. Share Creation Notification

To create a Share, the Sending Server SHOULD make a HTTP POST request

- * to the /shares path in the Receiving Server's OCM API
- * using application/json as the Content-Type HTTP request header
- * its request body containing a JSON document representing an object with the fields as described below
- * using TLS
- * using httpsig [RFC9421]

6.1. Fields

- * REQUIRED shareWith (string) OCM Address of the user, group or federation the provider wants to share the Resource with. This MUST be known in advance, either via a previous Invitation or through other means. Example:
"51dc30ddc473d43a6011e9ebba6ca770@geant.org"
- * REQUIRED name (string) Name of the Resource (file or folder). Example: "resource.txt"
- * OPTIONAL description (string) Optional description of the Resource (file or folder). Example: "This is the Open API Specification file (in YAML format) of the Open Cloud Mesh API."
- * REQUIRED providerId (string) Opaque value to identify the Shared Resource at the provider side. This MUST be unique per Resource and per share, such that multiple shares of a given Resource are guaranteed to get different values. Example:
7c084226-d9a1-11e6-bf26-cec0c932ce01
- * REQUIRED owner (string) - OCM Address of the user who owns the Resource. Example: "6358b71804dfa8ab069cf05ed1b0ed2a@apiwise.nl"
- * REQUIRED sender (string) - OCM Address of the user that wants to share the Resource. Example:
"527bd5b5d689e2c32ae974c6229ff785@apiwise.nl"
- * OPTIONAL ownerDisplayName (string) Display name of the owner of the Resource Example: "Dimitri"
- * OPTIONAL senderDisplayName (string) Display name of the user that wants to share the Resource Example: "John Doe"

- * REQUIRED shareType (string) SHOULD have a value of "user", "group", or "federation", to indicate that the first part of the shareWith OCM Address refers to a Receiving Party who is a single user of the Receiving Server, a group of users at the Receiving Server, or a group of users that spans multiple OCM Servers belonging to a federation as exposed by a Directory Service, including at least one user at the Receiving Server. In the federation case, OCM Servers MAY resolve the actual recipients by either querying external AAI systems, or exchanging the groups' metadata between themselves. Such exchange is out of scope for this version of the this specification. Alternatively, the Receiving Server MAY hold the federated groups' metadata and act as an OCM proxy, forwarding the OCM requests to the actual members of the federation.
- * REQUIRED resourceType (string) Resource type (file, folder, calendar, contact, ...). If the Resource is a folder, implementations SHOULD advertise it as folder rather than file, in order to streamline the processing by the Receiving Server.
- * OPTIONAL expiration (integer) The expiration time for the OCM share, in seconds of UTC time since Unix epoch. If omitted, it is assumed that the share does not expire. A sender server MAY use it to signal that the resource represents a cached copy of a dataset that was made available for an efficient data transfer to the destination server.
- * REQUIRED protocol (object) JSON object with specific options for each protocol. The supported protocols are: - webdav, to access the data - webapp, to access remote web applications - ssh, to access the data via a public/private key pair. Other custom protocols might be added in the future. In case a single protocol is offered, there are three ways to specify this object: Option 1: Set the name field to the name of the protocol, and put the protocol details in a field named options. Option 2: Set the name field to the name of the protocol, and put the protocol details in a field carrying the name of the protocol. Option 3: Set the name field to multi, and put the protocol details in a field carrying the name of the protocol. Option 1 using the options field is now deprecated. Implementations are encouraged to transition to the new optional properties defined below, such that this field may be removed in a future major version of the spec. When specifying more than one protocol as different ways to access the Share, the name field needs to be set to multi. If multi is given, one or more protocol endpoints are expected to be defined according to the optional properties specified below. Otherwise, at least webdav is expected to be supported, and its options MAY be given in the opaque options payload for compatibility with v1.0

implementations (see examples). Note though that this format is deprecated. Warning: client implementers should be aware that v1.1+ servers MAY support both webdav and multi, but v1.0 servers MAY only support webdav.

* Protocol details for webdav MAY contain:

- OPTIONAL `accessTypes` (array of strings) - The type of access being granted to the remote resource. If omitted, it defaults to `['remote']`. A subset of:
 - o `remote` signals the recipient that the resource is available for remote access and interactive browsing.
 - o `datatx` signals the recipient that the resource is available for data transfer. If no expiration is given, the share is suitable e.g. for sync use-cases, whereas if an expiration date is set, the above clause MAY apply and the recipient SHOULD notify the sender upon completing the data transfer, in order to ease cache operations on the Sending Server. The recipient MAY delegate a third-party service to execute the data transfer on their behalf.
- REQUIRED `uri` (string) A URI to access the Remote Resource. The URI SHOULD be relative, in which case the prefix exposed by the `/.well-known/ocm` endpoint MUST be used. Absolute URIs are deprecated.
- REQUIRED `sharedSecret` (string) A secret to be used to access the Resource, such as a bearer token. To prevent leaking it in logs it MUST NOT appear in any URI.
- OPTIONAL `permissions` (array of strings) - The permissions granted to the sharee. A subset of:
 - o `read` allows read-only access including download of a copy.
 - o `write` allows create, update, and delete rights on the Resource.
 - o `share` allows re-share rights on the Resource.
- OPTIONAL `requirements` (array of strings) - The requirements that the sharee MUST fulfill to access the Resource. A subset of:

- o must-use-mfa requires the consumer to be MFA-authenticated. This MAY be used if the recipient provider exposes the enforce-mfa capability.
 - o must-exchange-token requires the recipient to exchange the given sharedSecret via a signed HTTPS request to the Sending Server's {tokenEndPoint} [RFC6749]. This MAY be used if the recipient provider exposes the exchange-token capability.
 - OPTIONAL size (integer) The size of the resource to be transferred, useful especially in case of datatx access type.
- * Protocol details for webapp MAY contain:
- REQUIRED uri (string) A URI to a client-browsable view of the Shared Resource, such that users MAY use the web applications available at the site. The URI SHOULD be relative, in which case the prefix exposed by the /.well-known/ocm endpoint MUST be used. Absolute URIs are deprecated.
 - REQUIRED viewMode (string) The permissions granted to the sharee. A subset of:
 - o view allows access to the web app in view-only mode.
 - o read allows read and download access via the web app.
 - o write allows full editing rights via the web app.
 - OPTIONAL sharedSecret (string) An optional secret to be used to access the remote web app, for example in the form of a bearer token.
- * Protocol details for ssh MAY contain:
- OPTIONAL accessTypes (array of strings) - The type of access being granted to the remote resource. If omitted, it defaults to ['remote']. A subset of:
 - o remote signals the recipient that the resource is available for remote access, e.g. via sshfs.
 - o datatx signals the recipient to transfer the resource from the given URI via scp. The recipient MAY delegate a third-party service to execute the data transfer on their behalf.

- REQUIRED uri (string) The full address to be used for ssh or scp access, in the form username@host.fqdn:port/resource/path, where the username is chosen by the Sending Server and does not necessarily need to match the recipient's OCM Address. Authentication is expected to take place via public/private key: the Receiving Server MUST reply to such a Share Creation Notification by sending back their public key, for the Sender Server to authorize access to the Resource.

6.2. Response

The Share Creation Notification Response SHOULD be a HTTP response:

- * in response to the Share Creation Notification Request
- * using application/json as the Content-Type HTTP response header

A 201 response status means the Share Creation Notification Request was successful. In this case, the response body MUST contain a JSON document representing an object with the following string fields: - REQUIRED: recipientDisplayName - the Recipient's display name. - OPTIONAL: recipientPublicKeys - the Recipient's public key(s). This property MUST be returned when the protocol of the incoming share was ssh. A 400 response status means some parameters were invalid or missing. A 401 response status means the Sender cannot be authenticated as a trusted service. A 403 response status means the Sender is not authorized to create shares. A 501 response status means either the Receiver does not support incoming external shares, or the share type or the resource type are not supported. A 503 response status means that the Receiver is temporary unavailable.

6.3. Decision to Discard

The Receiving Server MAY discard the notification if any of the following hold true:

- * the HTTP Signature is missing but the Sending Server does expose a keypair discoverable from the FQDN part of the sender field in the request body
- * the HTTP Signature is missing
- * the HTTP Signature is not valid
- * no keypair is trusted or discoverable from the FQDN part of the sender field in the request body

- * the keypair used to generate the HTTP Signature doesn't match the one trusted or discoverable from the FQDN part of the sender field in the request body
- * the Sending Server is denylisted
- * the Sending Server is not allowlisted
- * the Sending Party is not trusted by the Receiving Party (e.g., no Invite was exchanged and/or the Sending Party's OCM Address does not appear in the Receiving Party's address book)
- * the Receiving Server is unable to act as an API client for (any of) the protocol(s) listed for accessing the Resource
- * an initial check shows that the Resource cannot successfully be accessed through (any of) the protocol(s) listed

6.4. Receiving Party Notification

If the Share Creation Notification is not discarded by the Receiving Server, they MAY notify the Receiving Party passively by adding the Share to some inbox list, and MAY also notify them actively through for instance a push notification or an email message.

They could give the Receiving Party the option to accept or reject the share, or add the share automatically and only send an informational notification that this happened.

7. Share Acceptance Notification

In response to a Share Creation Notification, the Receiving Server MAY discover the OCM API of the Sending Server, starting from the <fqdn> part of the sender field in the Share Creation Notification.

If the OCM API of the Sending Server is successfully discovered, the Receiving Server MAY make a HTTP POST request

- * to the /notifications path in the Sending Server's OCM API
- * using application/json as the Content-Type HTTP request header
- * its request body containing a JSON document representing an object with the fields as described below
- * using TLS
- * using httpsig [RFC9421]

7.1. Fields

- * REQUIRED notificationType (string) - in a Share Acceptance Notification it MUST be one of:
 - 'SHARE_ACCEPTED'
 - 'SHARE_DECLINED'
- * REQUIRED providerId (string) - copied from the Share Creation Notification for the Share this notification is about
- * OPTIONAL resourceType (string) - copied from the Share Creation Notification for the Share this notification is about
- * OPTIONAL notification (object) - optional additional parameters, depending on the notification and the resource type

For example, a notification MAY be sent by a recipient to let the provider know that the recipient declined a share. In this case, the provider site MAY mark the share as declined for its user(s). Similarly, it MAY be sent by a provider to let the recipient know that the provider removed a given share, such that the recipient MAY clean it up from its database. A notification MAY also be sent to let a recipient know that the provider removed that recipient from the list of trusted users, along with any related share. The recipient MAY reciprocally remove that provider from the list of trusted users, along with any related share.

Notifications from Sending Server to Receiving Server SHOULD use httpsig [RFC9421] so the Receiving Server can authenticate the origin of the notification. Receiving Servers SHOULD decline notifications from Sending Servers without httpsig as it can't identify where the notification is coming from.

8. Resource Access

To access the Resource, the Receiving Server MAY use multiple ways, depending on the body of the Share Creation Notification and the protocol required for access. The procedure is as follows:

1. The receiver MUST extract the OCM Server FQDN from the sender field of the received share, and MUST query the Discovery (Section 5) endpoint at that address: let <sender-ocm-path> be the resourceTypes[0].protocols.webdav value to be used later, if defined.

2. If `protocol.name` is multi, the receiver MUST inspect the `protocol.{protocolName}` properties corresponding to the protocol of concern, and act according to its semantics. For the specific case where `protocol.webdav` is available and the receiver wants to use it, the following steps are to be followed.
3. The `protocol.webdav.requirements` MUST be inspected:
 - 3.1. If it includes `must-exchange-token`, the receiver MUST make a signed POST request to the path in the Sending Server's `{tokenEndPoint}`, to exchange the `protocol.webdav.sharedSecret` token for a short-lived bearer token, and only use that bearer token to access the Resource (See the Code Flow (Section 9) section). If the `must-exchange-token` requirement is not present and the Discovery endpoint inspected at step 1. exposes the token-exchange capability, the receiver MAY attempt to perform the token exchange as above, but it MUST fall back to the following steps should the process fail.
 - 3.2. If it includes `must-use-mfa`, the Receiving Server MUST ensure that the Receiving Party has been authenticated with MFA, or prompt the consumer in order to elevate their session, if applicable.
4. The `protocol.webdav.uri` property MUST now be inspected: if it's a complete URI, the receiver MUST make a HTTP PROPFIND request against it to access the Remote Resource, otherwise it is to be taken as an identifier `<id>`, in which case the receiver MUST make a HTTP PROPFIND request to: `https://<sender-host><sender-ocm-path>/<id>` in order to access to the Remote Resource. The receiver MUST pass an `Authorization: bearer` header with either the short-lived bearer token obtained in step 3.1., if applicable, or the `protocol.webdav.sharedSecret` value.
5. Otherwise, if `protocol.name` is `webdav` the receiver SHOULD inspect the `protocol.options.sharedSecret` property: if `protocol.options.sharedSecret` is defined, then the receiver SHOULD make a HTTP PROPFIND request to `https://<sharedSecret>:@<sender-host><sender-ocm-path>`. Note that this access method, based on Basic Auth, is `_deprecated_` and may be removed in a future release of the Protocol. If a secret cannot be identified (e.g. because `protocol.options` is undefined), then the receiver SHOULD discard the share as invalid.

In all cases, in case the Shared Resource is a folder and the Receiving Server accesses a Resource within that shared folder, it SHOULD append its relative path to that URL. In other words, the Sending Server SHOULD support requests to URLs such as `https://<sender-host><sender-ocm-path>/path/to/resource.txt`.

9. Code Flow

This section defines the procedure for issuing short-lived bearer access tokens for use by the Receiving Server when accessing a resource shared through OCM. The mechanism is aligned with the OAuth 2.0 `_authorization_code_` grant type but is performed entirely as a server to server interaction between the Sending and Receiving Servers. No user interaction or redirect is involved. [RFC6749]

9.1. Token Request

To obtain an access token, the Receiving Server MUST send an HTTP POST request to the Sending Server's `{tokenEndPoint}` as discovered in the OCM provider metadata, following section 4.4.2 of [RFC6749]. The request payload MUST be in `x-www-form-urlencoded` form, as shown in the following example (with line breaks in the Signature headers for display purposes only):

```
POST {tokenEndPoint} HTTP/1.1
Host: cloud.example.org
Date: Wed, 05 Nov 2025 14:00:00 GMT
Content-Type: application/x-www-form-urlencoded
Digest: SHA-256=ok6mQ3WZzKc8nb7s/Jt2yYluK7d2n8Zq7dhl3Q0slxk=
Content-Length: 101
Signature-Input:
  sig1=("@method" "@target-uri" "content-digest" "date");
  created=1730815200;
  keyid="receiver.example.org#key1";
  alg="rsa-sha256"
Signature: sig1=bM2sV2a4oM8pWc4Q8r9Zb8bQ7a2vH1kR9xT0yJ3uE4wO5lV6bZ1cP
  2rN3qD4tR5hC=:
```

```
grant_type=authorization_code&
client_id=receiver.example.org&
code=my_secret_code
```

The request MUST be signed using an HTTP Message Signature [RFC9421]. The `client_id` identifies the Receiving Server and MUST be set to its fully qualified domain name. The `code` parameter carries the authorization secret that was issued by the Sending Server in the Share Creation Notification. It is allowed to send the additional parameters defined in [RFC6749] for the `authorization_code` grant type, but they MUST be ignored.

9.2. Token Response

If the request is valid and the code is accepted, the Sending Server MUST respond with HTTP 200 OK and a OAuth-compliant JSON object containing the issued token:

```
{
  "access_token": "8f3d3f26-f1e6-4b47-9e3e-9af6c0d4ad8b",
  "token_type": "Bearer",
  "expires_in": 300
}
```

The access_token is an opaque bearer credential with no internal structure visible to the Receiving Server. The token authorizes the Receiving Server to access the shared resource using the appropriate transport protocol (e.g., WebDAV). The expires_in value indicates the token lifetime in seconds. No refresh_token is issued, instead the same request to the {tokenEndPoint} MUST be repeated before the access_token has expired, to receive a new access_token that can then be used in the same manner.

9.3. Error Responses

If the request is invalid, the Sending Server MUST return an HTTP 400 response with a JSON object containing an OAuth 2.0 error code [RFC6749]:

```
{ "error": "invalid_request" }
```

Permitted error codes are invalid_request, invalid_client, invalid_grant, unauthorized_client and unsupported_grant_type.

10. Share Deletion

A "SHARE_ACCEPTED" notification followed by a "SHARE_UNSHARED" notification is equivalent to a "SHARE_DECLINED" notification.

Note that the Sending Server MAY at any time revoke access to a Resource (effectively undoing or deleting the Share) without notifying the Receiving Server.

11. Share Updating

Some implementations have experimented with a "RESHARE_CHANGE_PERMISSION" notification, but the payload and side effects such a notification may have are out of scope of this version of this specification. The Receiving Party sending such a notification has no way of knowing if the Sending Party understood and processed the reshare request or not.

12. Resharing

The "REQUEST_RESHARE" and "RESHARE_UNDO" notification types MAY be used by the Receiving Server to persuade the Sending Server to share the same Resource with another Receiving Party. The details of the payload and side effects such a notification may have are out of scope of this version of this specification. Note that the Receiving Party sending such a notification has no way of knowing if the Sending Party understood and processed the reshare request or not. In all cases, the Receiving Server MUST NOT reshare a Resource without an explicit grant from the Sending Server.

13. IANA Considerations

13.1. Well-Known URI for the Discovery

The following value is to be registered in the "Well-Known URIs" registry (using the template from [RFC5785]): URI suffix: ocm Change controller: IETF Specification document(s): the present Draft, once in RFC form Related information: N/A

13.2. JSContact Types Registry

The following entry is to be registered in the "JSContact Types" registry (using the template from [RFC9553]): Type Name: ocmAddress Intended Usage: common Since Version: 1.0 Until Version: N/A Change Controller: IETF Reference or Description:

An object representing an OCM address. The object contains:

- "address" (String, required): The OCM federated address in format "user@provider" where provider is the FQDN of an OCM-capable server.
- "trusted" (Boolean, optional): Whether shares from this address are automatically accepted. Default: false.
- "source" (String, optional): How this address was established. See "JSContact Enum Values" registry for allowed values.
- "label" (String, optional): Human-readable label for this address.

13.3. JSContact Properties Registry

The following entry is to be registered in the "JSContact Properties" registry (using the template from [RFC9553]): Property Name: ietf.org:ocmAddresses Property Type: String[ocmAddress] Property Context: Card Intended Usage: common Since Version: 1.0 Until Version: N/A Change Controller: IETF Reference or Description:

A map of OCM addresses for a contact. The keys are arbitrary identifiers (e.g., "primary", "work") and the values are ocmAddress objects as defined in the JSContact Types Registry.

13.4. JSContact Enum Values Registry

The following entries are to be registered in the "JSContact Enum Values" registry (using the template from [RFC9553]). Property Name: ietf.org:ocmAddresses/source Context: Card Since Version: 1.0 Until Version: N/A Change Controller: IETF Reference or Description:

Values indicating how an OCM address was established.

Initial Contents:

Enum Value	Reference/Description
invite	Address established via OCM invite flow
share	Address established by receiving a share
direct entry	Address added directly by the user

14. Security Considerations

14.1. Trust

There are several areas that are not covered by this specification. Most importantly we do not provide a way of establishing trust between servers, even though some features of the protocol rely on trust, such as the mfa-enforced requirement.

Trust needs to be established out of band, but there are some features of the protocol that can be used to assist operators in establishing trust. For instance, invite flow can be used to establish that users know and have out of band connections with other users on an OCM server.

Further more the Directory Service feature can be used to establish a trusted federation, where a central authority can be trusted to implement measures for auditing and adding only trusted servers into the discovery service.

14.1.1. httpsig

It is RECOMMENDED to use signed messages, "httpsig" [RFC9421], to verify that an OCM server is the server you expect it to be, and SHOULD be done unless you have a niche use case.

14.2. Legacy shared secrets

The legacy format of an OCM Share Notification with shared secrets is only provided for backwards compatibility with existing implementations. Implementers SHOULD NOT use it and prefer short-lived tokens instead.

14.3. Code Flow

All {tokenEndPoint} requests MUST be transmitted over HTTPS and signed using HTTP Signatures. Bearer tokens MUST be treated as confidential and never logged, persisted beyond their lifetime, or transmitted over unsecured channels.

15. References

15.1. Normative References

[RFC2119] Bradner, S. "Key words for use in RFCs to Indicate Requirement Levels (<https://datatracker.ietf.org/doc/html/rfc2119>)", March 1997.

[RFC3986] Berners-Lee, T., Fielding, R. and Masinter, L. "Uniform Resource Identifier (URI): Generic Syntax (<https://datatracker.ietf.org/doc/html/rfc3986>)", January 2005

[RFC4918] Dusseault, L. M. "HTTP Extensions for Web Distributed Authoring and Versioning (<https://datatracker.ietf.org/html/rfc4918/>)", June 2007.

[RFC6749] Hardt, D. (ed), "The OAuth 2.0 Authorization Framework (<https://datatracker.ietf.org/html/rfc6749>)", October 2012.

[RFC7515] Jones, M., Bradley, J., Sakimura, N., "JSON Web Signature (JWS) (<https://datatracker.ietf.org/doc/html/rfc7515>)", May 2015.

- [RFC7517] Jones, M., "JSON Web Key (JWK) (<https://datatracker.ietf.org/doc/html/rfc7517>)", May 2015.
- [RFC8032] Josefsson, S., Liusvaara, I., "Edwards-Curve Digital Signature Algorithm (EdDSA) (<https://datatracker.ietf.org/doc/html/rfc8032>)", January 2017.
- [RFC8174] Leiba, B. "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words (<https://datatracker.ietf.org/html/rfc8174>)", May 2017.
- [RFC8615] Nottingham, M. "Well-Known Uniform Resource Identifiers (URIs) (<https://datatracker.ietf.org/doc/html/rfc8615>)", May 2019
- [RFC9421] Backman, A., Richer, J. and Sporny, M. "HTTP Message Signatures (<https://tools.ietf.org/html/rfc9421>)", February 2024.
- [RFC9553] Stepanek, R., Loffredo, M., "JSContact: A JSON Representation of Contact Data (<https://datatracker.ietf.org/doc/html/rfc9553>), May 2024"

16. Appendix A: Multi-factor Authentication

If a Receiving Server exposes the capability `enforce-mfa`, it indicates that it will try and comply with a MFA requirement set on a Share. If the Sending Server trusts the Receiving Server, the Sending Server MAY set the requirement `mfa-enforced` on a Share, which the Receiving Server MUST honor. A compliant Receiving Server that signals that it is MFA-capable MUST NOT allow access to a Resource protected with the `mfa-enforced` requirement, if the Receiving Party has not provided a second factor to establish their identity with greater confidence.

Since there is no way to guarantee that the Receiving Server will actually enforce the MFA requirement, it is up to the Sending Server to establish a trust with the Receiving Server such that it is reasonable to assume that the Receiving Server will honor the MFA requirement. This establishment of trust will inevitably be implementation dependent, and can be done for example using a pre approved allow list of trusted Receiving Servers. The procedure of establishing trust is out of scope for this specification: a mechanism similar to the ScienceMesh (<https://sciencemesh.io>) integration for the Invite (Section 4.4) capability may be envisaged.

17. Appendix B: JWKS and HTTP Signature Examples

17.1. JWKS Endpoint

An OCM Server that advertises the http-sig capability MUST expose its public keys at `/.well-known/jwks.json` in the format specified by [RFC7517]. Here is an example response from `https://sender.example.org/.well-known/jwks.json`:

```
{
  "keys": [
    {
      "kty": "OKP",
      "crv": "Ed25519",
      "kid": "sender.example.org#key1",
      "x": "11qYAYKxCrfVS_7TyWQH0g7hcvPapiMlrwIaaPcHURo"
    }
  ]
}
```

17.2. Signing a Request (Sender)

Given a Share Creation Notification request:

```
POST /ocm/shares HTTP/1.1
Host: receiver.example.org
Date: Fri, 16 Jan 2026 13:37:00 GMT
Content-Type: application/json
Content-Digest: sha-256=:LkpHyFOVbBDPxc7YbHDOWNzAv88qWuVfLNf4TUf9Uo8=:
```

```
{
  "shareWith": "marie@receiver.example.org",
  "name": "spec.yaml",
  "providerId": "7c084226-d9a1-11e6-bf26-cec0c932ce01",
  "owner": "einstein@sender.example.org",
  "sender": "einstein@sender.example.org",
  "ownerDisplayName": "Albert Einstein",
  "senderDisplayName": "Albert Einstein",
  "shareType": "user",
  "resourceType": "file",
  "protocol": {
    "name": "multi",
    "webdav": {
      "uri": "spec.yaml",
      "sharedSecret": "hfiuhworzwnur98d3wjiwahr",
      "permissions": ["read", "write"]
    }
  }
}
```

The signature base is constructed according to [RFC9421] (with line breaks in @signature-params for display purposes only):

```
"@method": POST
"@target-uri": https://receiver.example.org/ocm/shares
"content-digest": sha-256=: [digest-value] =:
"@signature-params": ("@method" "@target-uri" "content-digest");
    created=[timestamp];
    keyid="sender.example.org#key1";
    alg="ed25519"
```

Sign this base using for example Ed25519 ([RFC8032]) to produce the signature, then add headers (line breaks for display purposes only):

```
Signature-Input: sig1=("@method" "@target-uri" "content-digest");
    created=[timestamp];
    keyid="sender.example.org#key1";
    alg="ed25519"
Signature: sig1=: [signature-value] =:
```

17.3. Verifying a Signature (Receiver)

To verify an incoming signed request:

1. Extract the provider domain from the sender field in the request body
2. Fetch the public key from `https://<provider-domain>/.well-known/jwks.json`
3. Extract keyid from Signature-Input header and find the key matching the kid value in the [RFC7517] response
4. Reconstruct the signature base from the request using the components listed in Signature-Input as specified in [RFC9421]
5. Verify the signature using the appropriate algorithm (e.g., Ed25519 [RFC8032])

17.4. Validating the Payload

Following the validation of the signature, the host SHOULD also confirm the validity of the payload, that is ensuring that the actions implied in the payload actually initiated on behalf of the source of the request.

As an example, if the payload is about initiating a new share, the file owner has to be an account from the instance at the origin of the request.

18. Appendix C: Directory Service

A third-party Directory Service is a back-end service used to federate multiple OCM Servers and facilitate the Invite flow. It is expected to expose, via anonymous HTTPS GET, a signed JWS document [RFC7515], where the signing key MUST be made available offline and the payload MUST adhere to the following format:

- * REQUIRED: federation - a human-readable name for the list of OCM Servers exposed by the Directory Service
- * REQUIRED: servers - a JSON array of objects to describe the list of OCM Servers with the following string fields:
 - REQUIRED: url - an absolute URL identifying the OCM Server. It MUST:
 - o include scheme: either https:// or (for testing purposes) http://
 - o include host (either a FQDN or an IP address)
 - o MAY include a non-default port
 - o MUST NOT include a base path (e.g., /ocm)
 - o MUST NOT include userinfo, query, or fragment
 - REQUIRED: displayName - a human-readable name for the OCM Server Example:

```
{
  "payload": {
    "federation": "The ScienceMesh Directory",
    "servers": [
      {
        "url": "https://ocm-server-1.example.org",
        "displayName": "OCM Server 1"
      },
      {
        "url": "https://ocm-server-2.example.org:4443",
        "displayName": "OCM Server 2"
      },
      {
        "url": "http://192.168.1.1:8080",
        "displayName": "OCM Server 3"
      }
    ]
  },
  "protected": {"alg": "RS256"},
  "signature": "..."
}
```

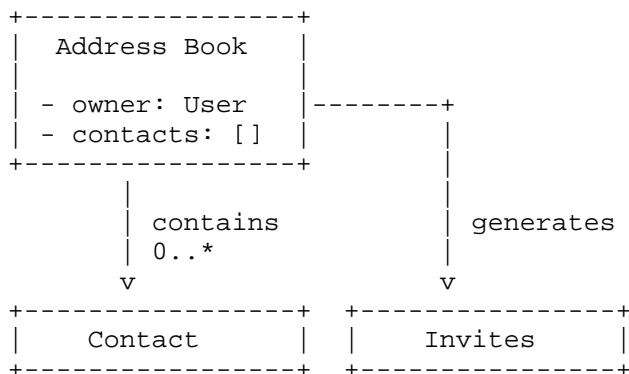
19. Appendix D: Object models

An implementor of OCM MAY choose any internal object model to represent an `_Address Book_`, a `_Contact_`, an `_Invite_`, a `_Provider_`, a `_Share_`, and a `_User_`. The following diagrams are provided to clarify the concepts and their relationships, as a guide for implementors.

19.1. Address Book

An `_OCM Provider_` MAY offer its `_Users_` an address book tool, where OCM Addresses can be stored over time in a labeled and/or searchable way. This decouples the act by which the OCM Address string is passed into the Sending Server's database from the selection of the `_Receiving Party_` in preparation for Share Creation.

The Address Book entity maintains a collection of contacts for a user within the OCM provider. It serves as the primary mechanism for managing federated relationships between users across different OCM Servers. `_Contacts_` may be added to the Address Book through the Invite flow or direct entry. It provides a convenient way for users to organize and access their federated contacts, and MAY allow users to generate `_Invites_`.



19.1.1.1. Properties

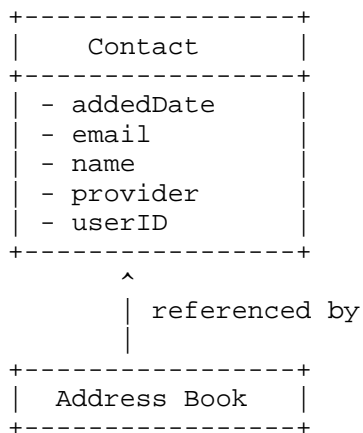
- * ***owner***: Reference to the User who owns this address book
- * ***contacts***: Array of Contact objects stored in the address book

19.1.1.2. Relationships

- * An Address Book belongs one or more Users.
- * An Address Book contains zero or more Contacts.
- * An Address Book MAY allow its owner to generate Invites.

19.2. Contact

A Contact represents a federated user relationship established through the OCM protocol. Contacts are stored in `_Address Books_` and may be created through the Invite process or via direct entry. A Contact MAY of course contain much more detailed information about the referenced user such as if it was added via `_Invites_` or direct entry.



19.2.1. Properties

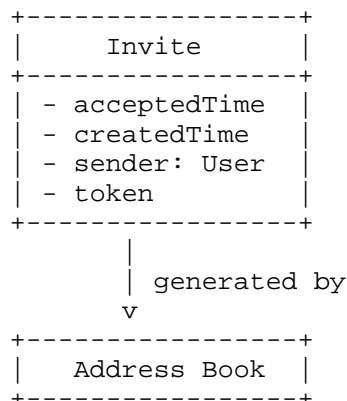
- * ***addedDate***: Timestamp of when contact was added
- * ***email***: Contact email address (informational)
- * ***name***: Human-readable display name
- * ***userID***: The identifier of the contact at their OCM Server
- * ***provider***: The FQDN of the contact's OCM Server

19.2.2. Relationships

- * A Contact may be referenced by one or more Address Books.

19.3. Invite

The Invite entity represents the bidirectional trust establishment mechanism in OCM. It facilitates secure contact exchange between users on different OCM Servers.



19.3.1. Properties

- * ***acceptedTime***: Timestamp of invite acceptance (if accepted)
- * ***createdTime***: Timestamp of invite creation
- * ***sender***: Reference to the User who sent the Invite
- * ***token***: Unique, hard-to-guess string generated by Invite Sender OCM Server

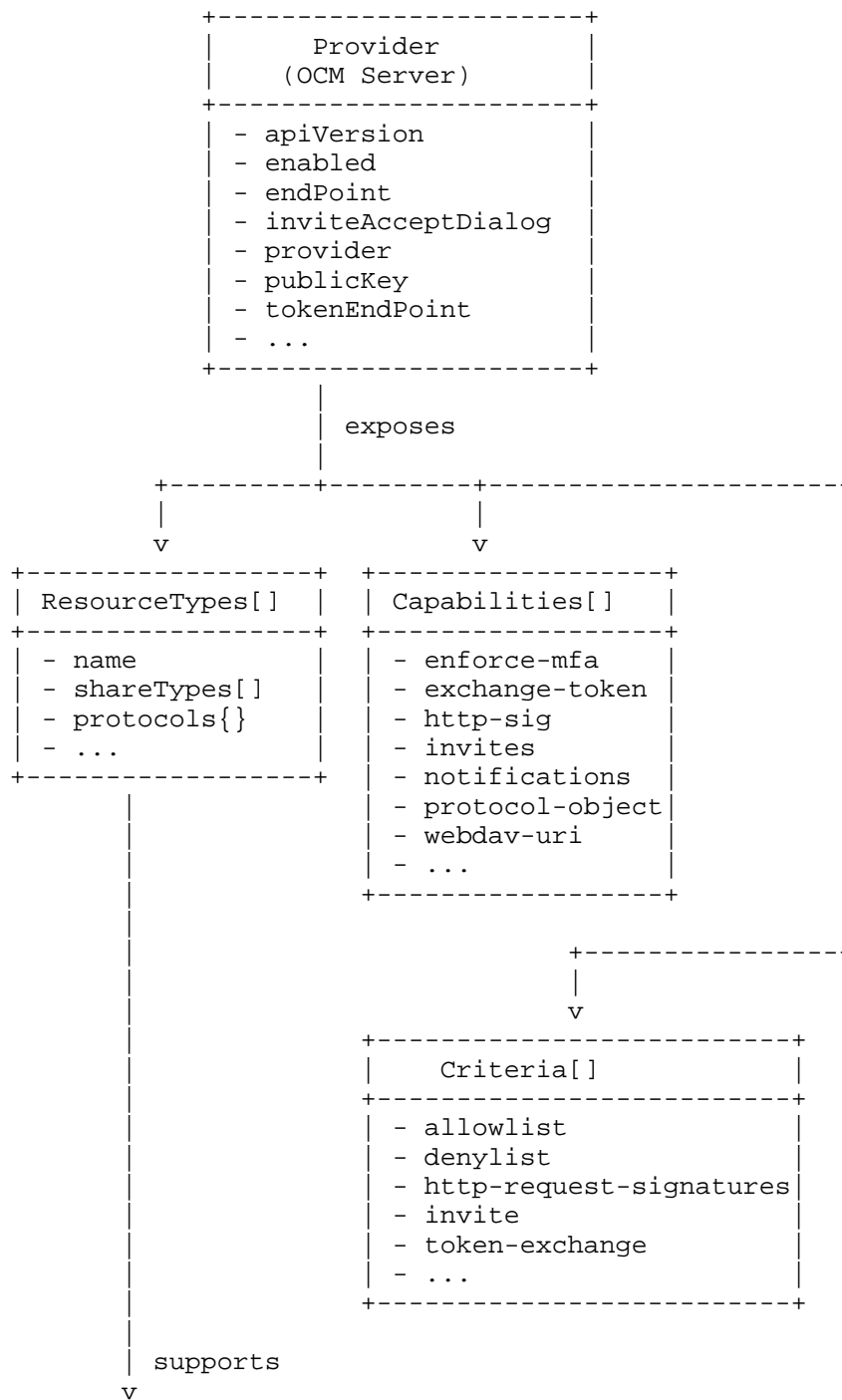
19.3.2. Relationships

- * An Invite is generated by an Address Book entry action.
- * An Invite is associated with exactly one User as the sender.

19.4. Provider

The Provider entity represents an OCM Server's capabilities and configuration as discovered through the OCM API Discovery process. It represents both the Sending Server and Receiving Server roles, and an implementor might find it useful to have a Provider object model to store the discovered information about federation peers or other remote OCM Providers.

The following diagram is illustrative and non-exhaustive. The single source of truth for Provider properties is the OCM API Discovery Fields section; for the box contents below, see the Properties subsection and the normative capability, criteria, and resource type definitions in that section.



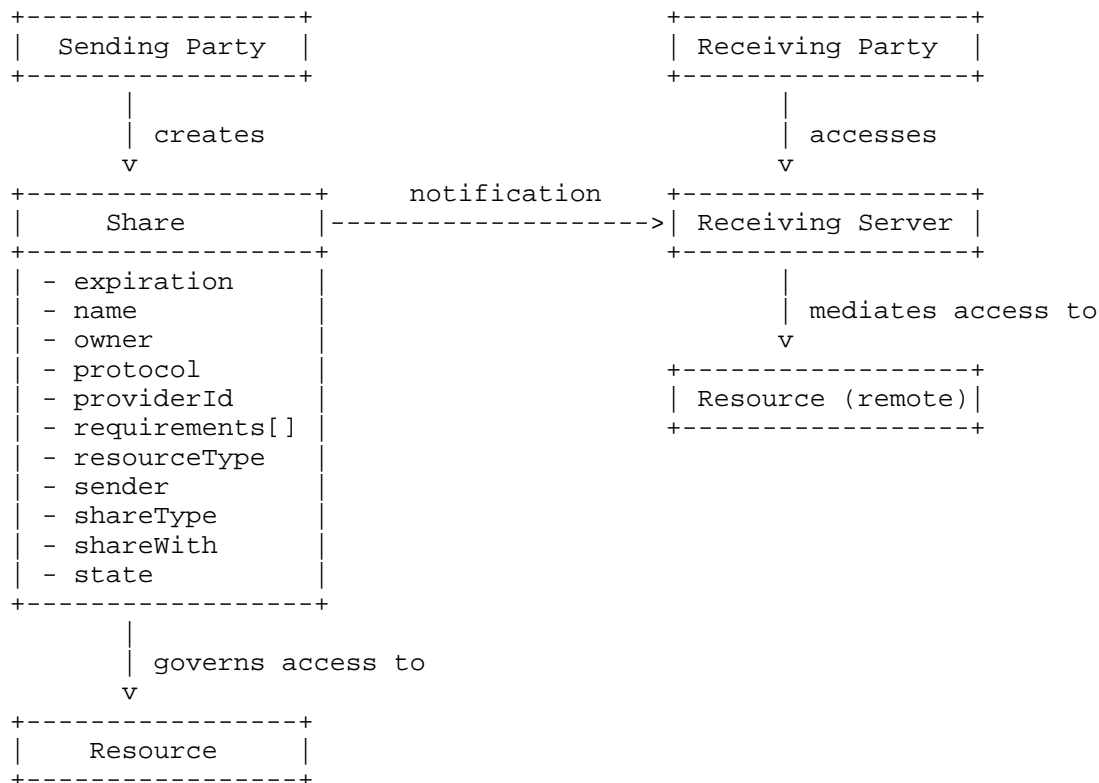
Protocols
<ul style="list-style-type: none">- ssh- webapp- webdav- ...

19.4.1. Properties

- * ***apiVersion***: Version string of supported OCM API
- * ***capabilities***: Optional features supported
- * ***criteria***: Requirements for accepting Share Creation Notifications
- * ***enabled***: Boolean indicating if OCM service is active
- * ***endpoint***: Base URI for OCM API endpoints
- * ***provider***: Friendly branding name
- * ***publicKey***: Optional public key for HTTP signatures
- * ***resourceTypes***: Array of supported resource types with protocols

19.5. Share

The Share entity represents a policy granting access to a `_Resource_` from a Sending Party to a Receiving Party.



19.5.1. Properties

- * ***expiration***: Optional expiration timestamp
- * ***name***: Human-readable name of the shared Resource
- * ***owner***: OCM Address of the Resource owner
- * ***protocol***: Access protocol name and details (webdav, ssh, webapp)
- * ***providerId***: Unique identifier for the Share at the provider
- * ***requirements***: Array of access requirements (must-use-mfa, must-exchange-token)
- * ***resourceType***: Type of resource (file, folder, calendar, etc.)
- * ***sender***: OCM Address of the party creating the Share
- * ***shareType***: Type of recipient (user, group, federation)

- * ***shareWith***: OCM Address of the Receiving Party
- * ***state***: Current state of the Share (accepted, pending, deleted)

19.5.1.1. Share States

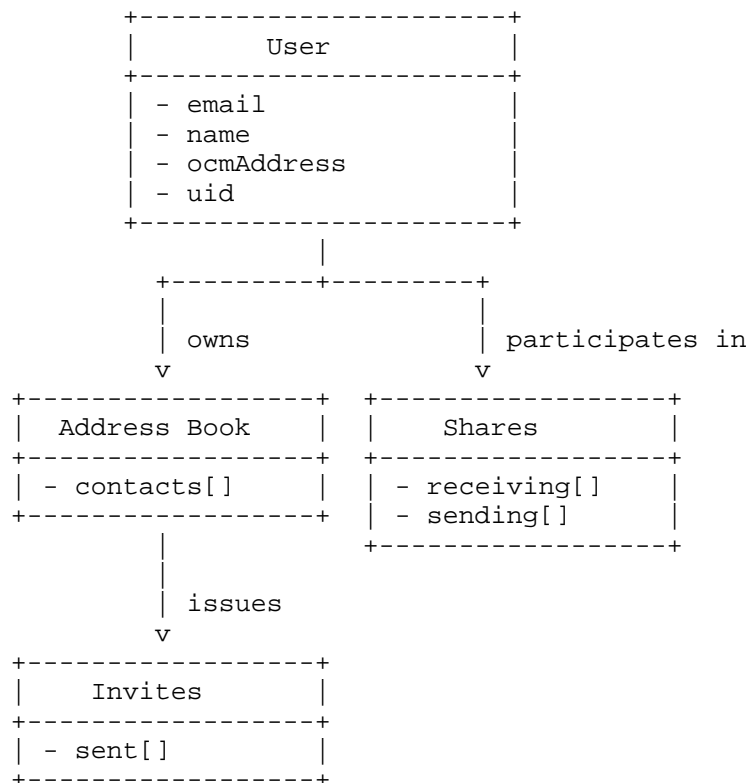
- * ***Accepted***: Share accepted, Resource accessible
- * ***Deleted***: Share removed or expired
- * ***Pending***: Awaiting acceptance by Receiving Party

19.5.2. Relationships

- * A Share is created by a User (local).
- * A Share is received by a User (remote).
- * A Share governs access to a Resource.

19.6. User

The User entity represents the party in OCM who can send and receive Shares and Invites and manage Contacts, and interact with Resources.



19.6.1. Properties

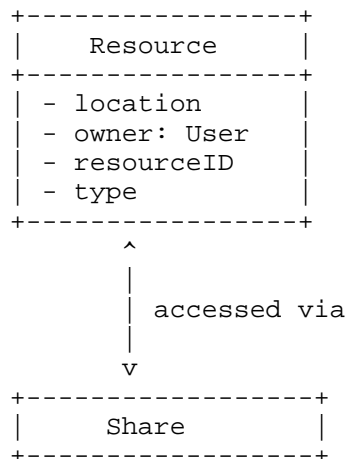
- * ***email***: User's email address
- * ***name***: Human-readable display name
- * ***ocmAddress***: Full OCM Address
- * ***uid***: Unique identifier within the OCM Provider

19.6.2. Relationships

- * A User owns one or more Address Book(s).
- * A User issues zero or more Invites.
- * A User participates in zero or more Shares as Sending or Receiving Party.

19.7. Resource

The Resource entity represents the data or service being shared between OCM Providers. It is the target of Shares and is accessed by the Receiving Party through the Sending Server's API. In general a Resource is a much more complex entity, but for the purpose of OCM we only need to model a few key properties.



19.7.1. Properties

- * ***location***: URI or path to access the Resource
- * ***owner***: Reference to the User who owns the Resource
- * ***resourceID***: Unique identifier of the Resource
- * ***type***: Type of Resource (file, folder, calendar, etc.)

20. Changes

This section collects the changes with respect to the previous version in the IETF datatracker. It is meant to ease the review process and it shall be removed when going to RFC last call. The complete changelog is updated in the OCM-API GitHub repository.

20.1. Version 04

- * Clarified that the diagrams in Appendix D are illustrative and not normative.
- * Minor formatting fixes.

20.2. Version 03

- * Fixed formatting of artworks, code blocks and bullet lists.

20.3. Version 02

- * Added the `_Changes_` section.

20.4. Version 01

- * Introduced functions, roles, and object models to the specification.
- * Added support for SSH as a share access method.
- * Introduced `accessType` property in shares and removed the `dataTx` "protocol" in favor of a cleaner access model.
- * Improved resource access description with token exchange, and specified request payload format for the `/token` endpoint.
- * Added RFC 9421 HTTP Message Signatures support via `http-sig` capability and RFC 7515 (JWS) compliant JWKS and prescribed use of JWS for the Directory Service.
- * Updated and homogenized capabilities across the specification.
- * Added JSContact extension to IANA Considerations.
- * Changed example domain to use `cloud.example.org` per RFC 2606.

21. Acknowledgements

Our deepest thanks and appreciation go to the people who started the work on what would become this specification in 2015. In particular we want to thank (in alphabetical order) Guido Aben, Russell Albert, Holger Angenent, David Anto, Hrachya Astsatryan, Kurt Bauer, Charles du Jeu, Andreas Eckey, David Gillard, Andranik Hayrapetyan Wahi, Dimitri van Hees, Christoph Herzog, David Jericho, Frank Karlitschek, Christian Kracher, Ralph Krimmel, Massimo Lamanna, Simon Leinen, Jari Miettinen, Jakub Moscicki, Frederik Orellana, Vlad Roman, Christian Schmitz, Woojin Seok, Rogier Spoor, Christian Sprajc, Peter Szegedi, Ron Trompert, Benedikt Wegmann and Jonathan Xu.

We would also like to thank Ishank Arora, Gianmaria Del Monte, Jörn Friedrich Dreyer, Richard Freitag, Hugo González Labrador, Matthias Kraus, Maxence Lange, Lovisa Lugnegård, Sandro Mesterheide, Antoon Prins and Björn Schiele for their direct contributions to the specification.

Over the years many more people have been involved in the development of OCM. We would like to thank all of them for their contributions, including Jean-Thomas Acquaviva, Samuel Alfageme Sainz, Karsten Asshauer, Miroslav Bauer, Felix Bhm, Maciej Brzeniak, Diogo Castro, Gavin Charles Kennedy, Jarosław Czub, Milan Danecek, Michael D'Silva, Łukasz Dutka, Pedro Ferreira, Renato Furter, Klaas Freitag, Raman Ganguly, Eva Gergely, Hilary Goodson, Daniel Halbe, Dave Heyns, Jan Holesovsky, Jan Hornicek, Carina Kemp, Fergus Kerins, Andreas Klotz, Matthias Knoll, Christian Kracher, Mario Lassnig, Claudius Laumanns, Anthony Leroy, Patrick Maier, Vladislav Makarenko, Anna Manou, Rita Meneses, Zheng Meyer-Zhao, Crystal Michelle Chua, Yoann Moulin, Daniel Müller, Frederik Müller, Rasmus Munk, Micha Orzechowski, Jacek Paweł Kitowski, Iosif Peterfi, Alessandro Petraro, René Ranger, Angelo Romasanta, David Rousse, Carla Sauvanaud, Klaus Scheibenberger, Marcin Sieprawski, Tilo Steiger, C.D. Tiwari, Alejandro Unger and Tom Wezepoel.

Authors' Addresses

Giuseppe Lo Presti
CERN
Email: giuseppe.lopresti@cern.ch
URI: <https://cern.ch/lopresti>

Michiel de Jong
Ponder Source
Email: michiel@pondersource.org
URI: <https://pondersource.com>

Mahdi Baghbani
Ponder Source
Email: mahdi@pondersource.org
URI: <https://pondersource.com>

Micke Nordin
SUNET
Email: kano@sunet.se
URI: <https://code.smolnet.org/micke>