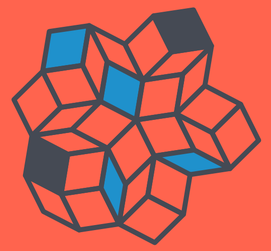
# Towards Standardisation

# Funding (gap year)

GÉANT



Science Mesh

NGI

?

OPENCLOUDMESH

# Authorization Flows

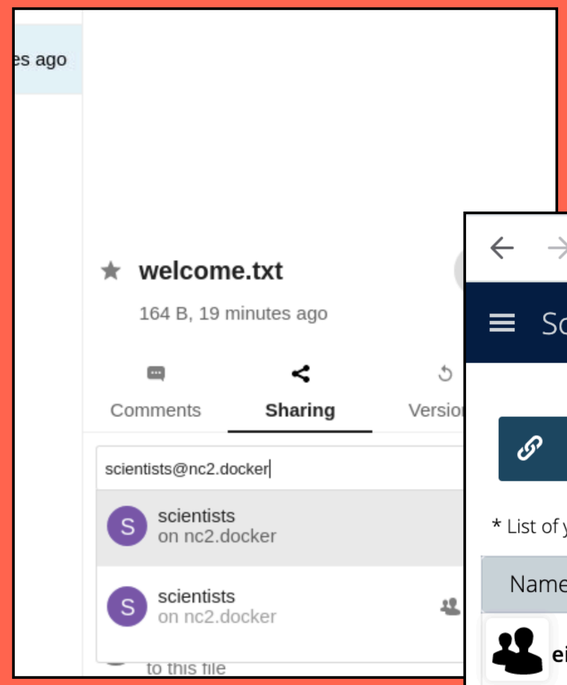
## Share-With

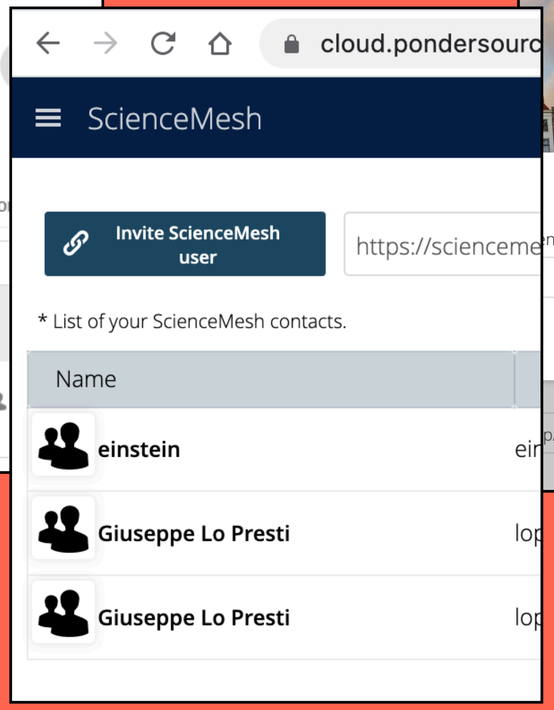
## Public Link

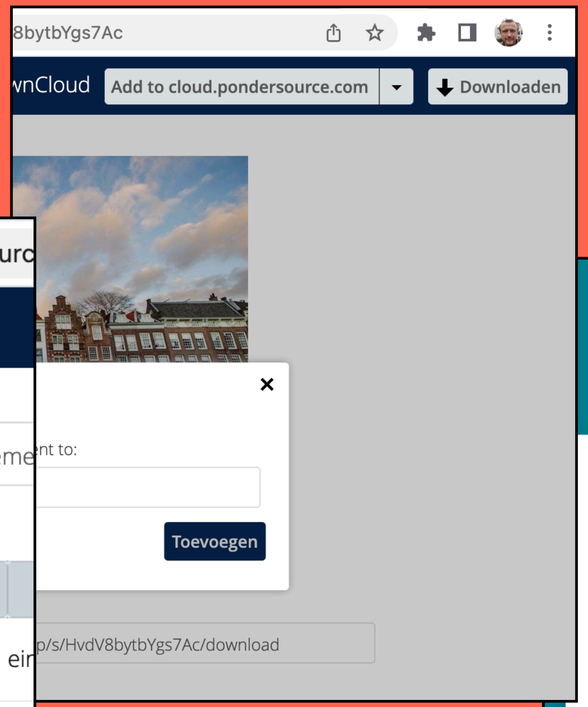
## Solid

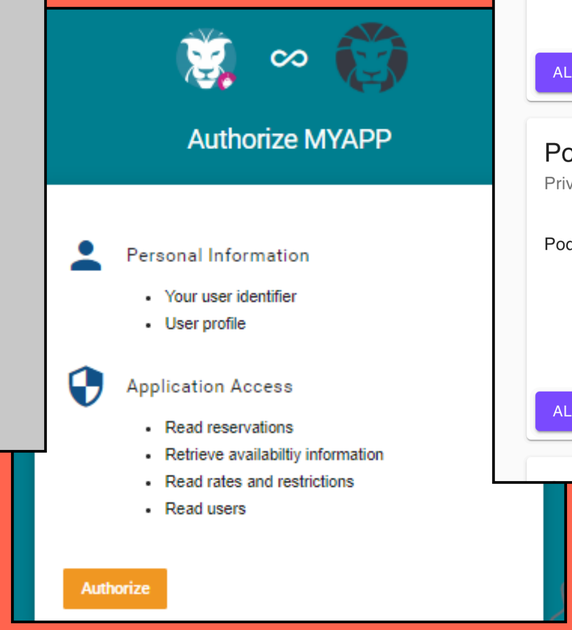
## Invite

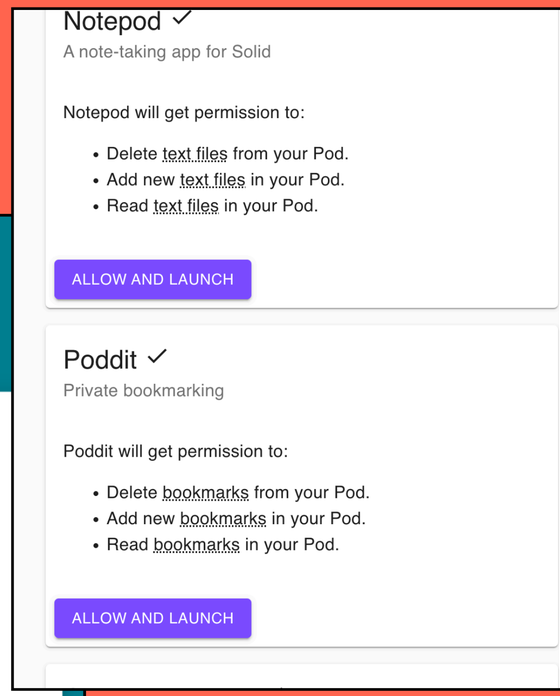
## OAuth



# OAuth Extension?


# draft-lopresti-open-cloud-mesh-00



| | |
|---|---|
| Workgroup: | Network Working Group |
| Internet-Draft: | draft-lopresti-open-cloud-mesh-00 |
| Published: | 15 November 2024 |
| Intended Status: | Standards Track |
| Expires: | 19 May 2025 |



| Authors: | G. Lo Presti | M. B. de Jong | M. Baghbani | M. Nordin |
|---|---|---|---|---|
| | *CERN* | *Ponder Source* | *Ponder Source* | *SUNET* |


## Open Cloud Mesh


### Abstract

Open Cloud Mesh 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.

Open Cloud Mesh only handles the necessary interactions up to the point where the Receiving Party is informed that they were granted access to the Resource. The actual resource access is then left to protocols such as WebDAV and others.


### 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 19 May 2025.

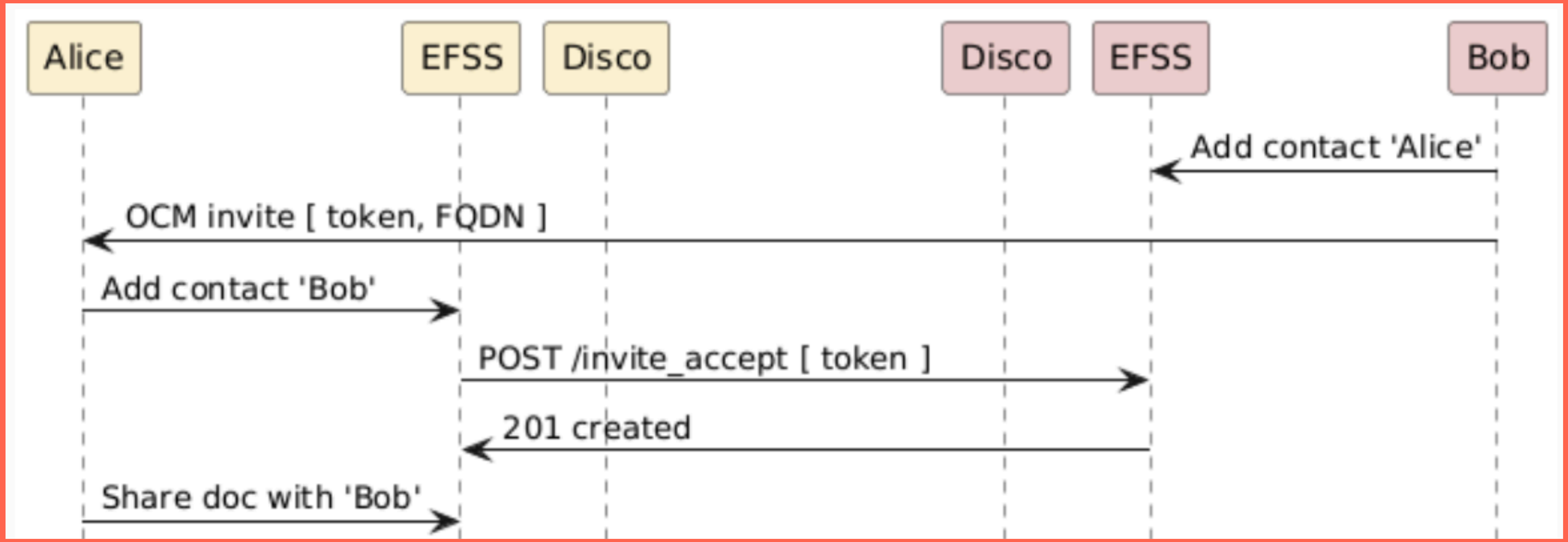


### 1. Terms

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

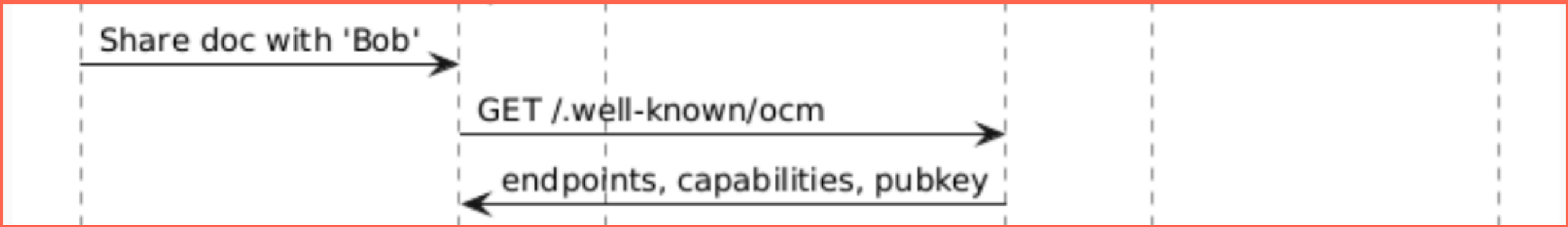
Table of Contents

# Invites help servers trust each other

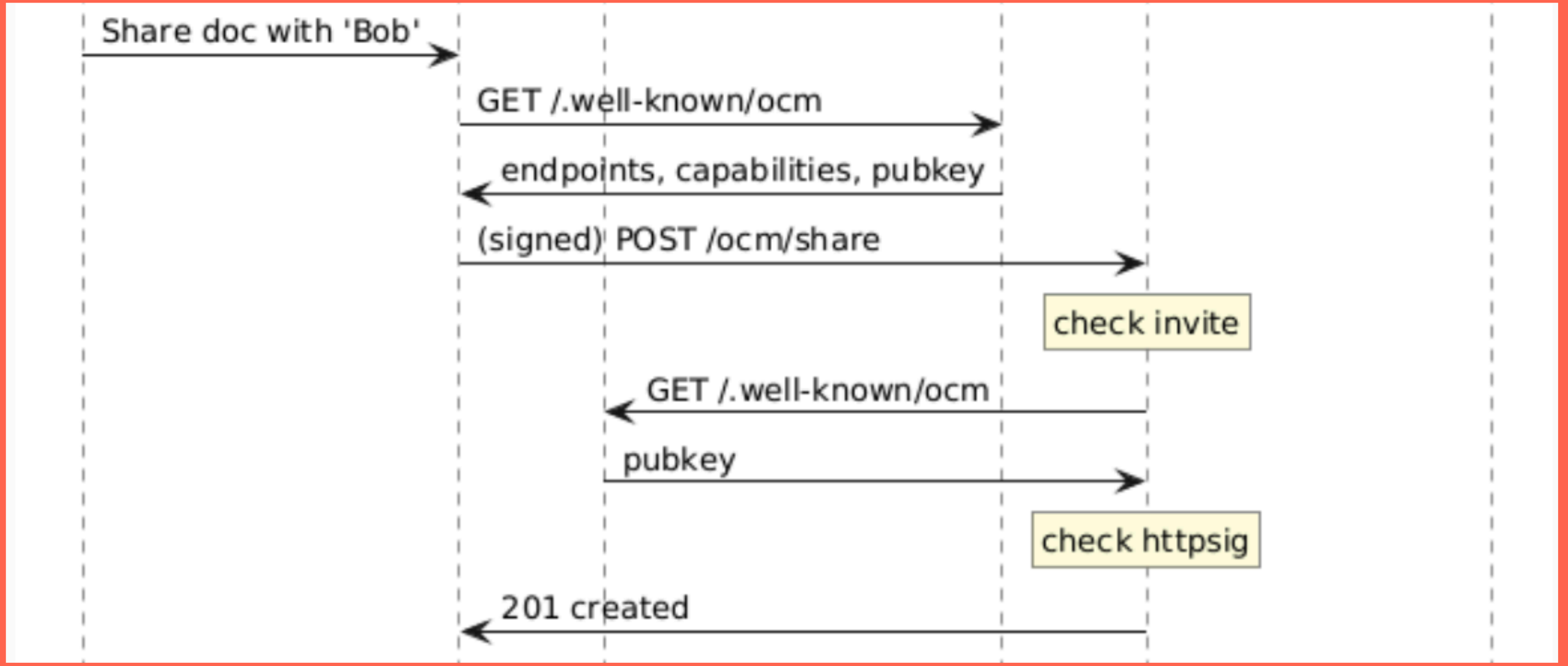


# Caps Disco

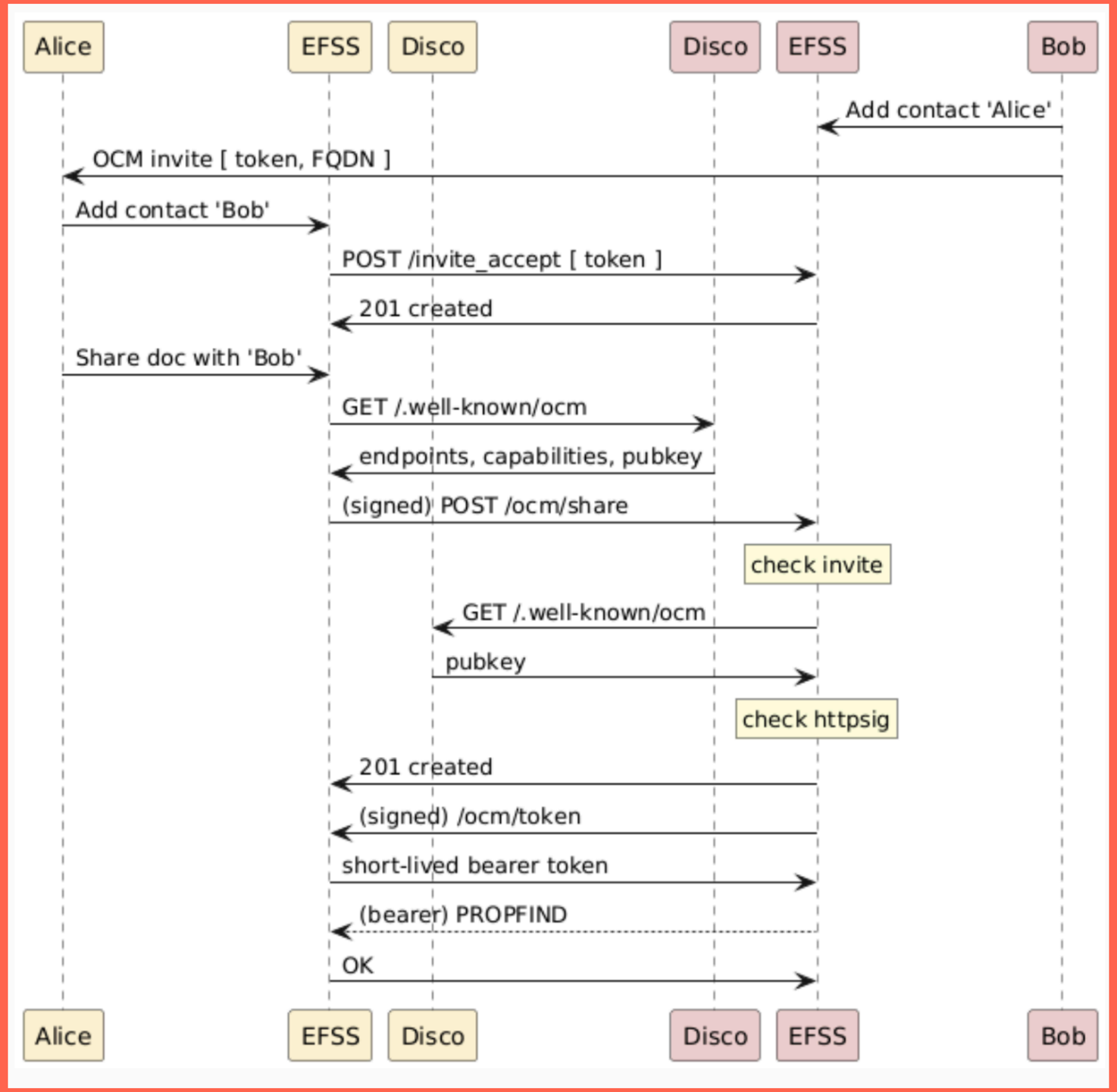
# Caps Disco


Share doc with 'Bob'
GET /.well-known/ocm
endpoints, capabilities, pubkey

# Share Creation Notification



# Exchange Code for Token


Alice
EFSS
Disco
Disco
EFSS
Bob
Add contact 'Alice'
OCM invite [ token, FQDN ]
Add contact 'Bob'
POST /invite_accept [ token ]
201 created
Share doc with 'Bob'
GET /.well-known/ocm
endpoints, capabilities, pubkey
(signed) POST /ocm/share
check invite
GET /.well-known/ocm
pubkey
check httpsig
201 created
(signed) /ocm/token
short-lived bearer token
(bearer) PROPFIND
OK
Alice
EFSS
Disco
Disco
EFSS
Bob

# THINGS TO ADD

- /ocm-provider to /.well-known/ocm
- protocol as keyed object in share
- webdav-uri path in share
- invites!
- group shares, federation shares
- enforce-mfa
- httpsig message signing
- code flow