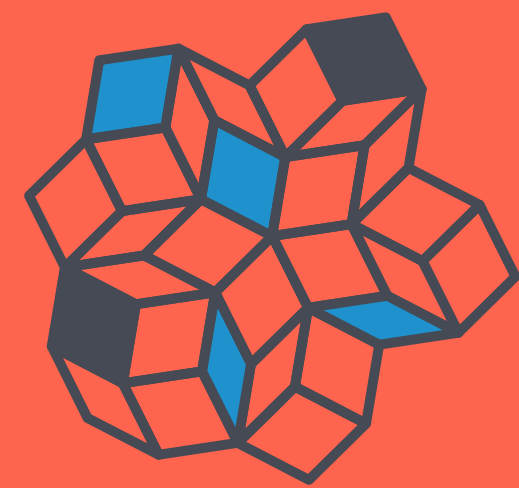




Towards Standardisation

Funding (gap year)



Science
Mesh

NGI

?



OPENCLOUDMESH

Authorization Flows

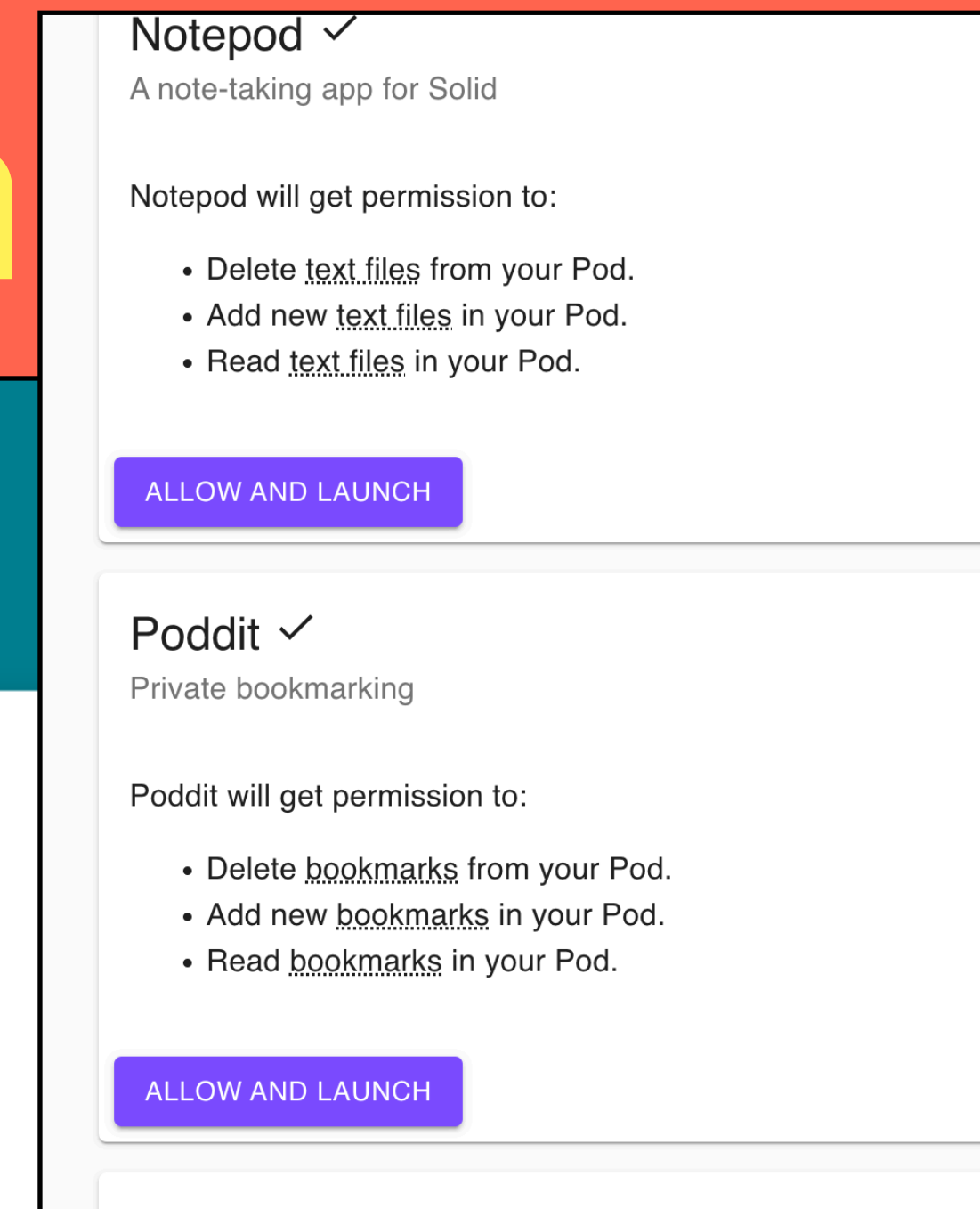
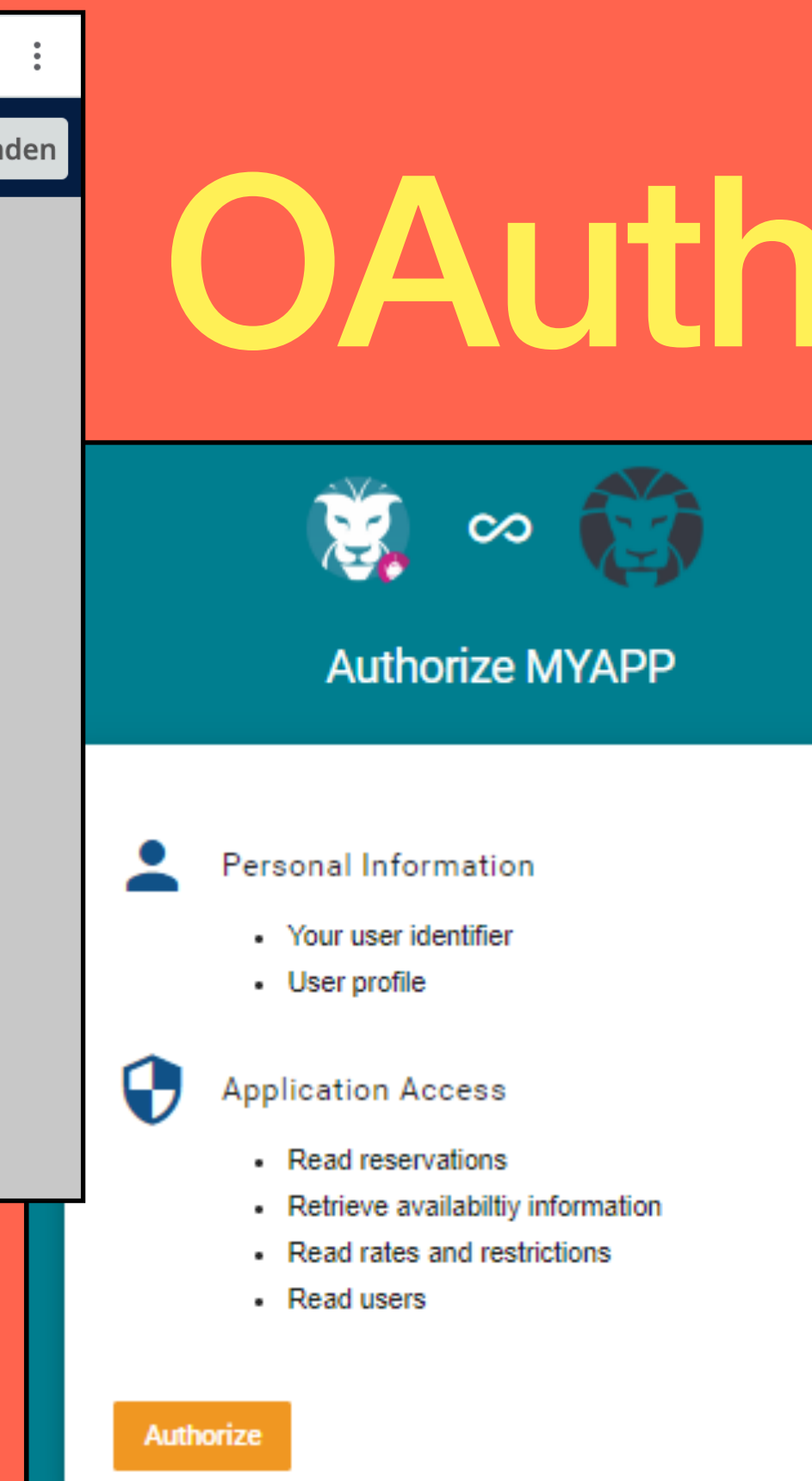
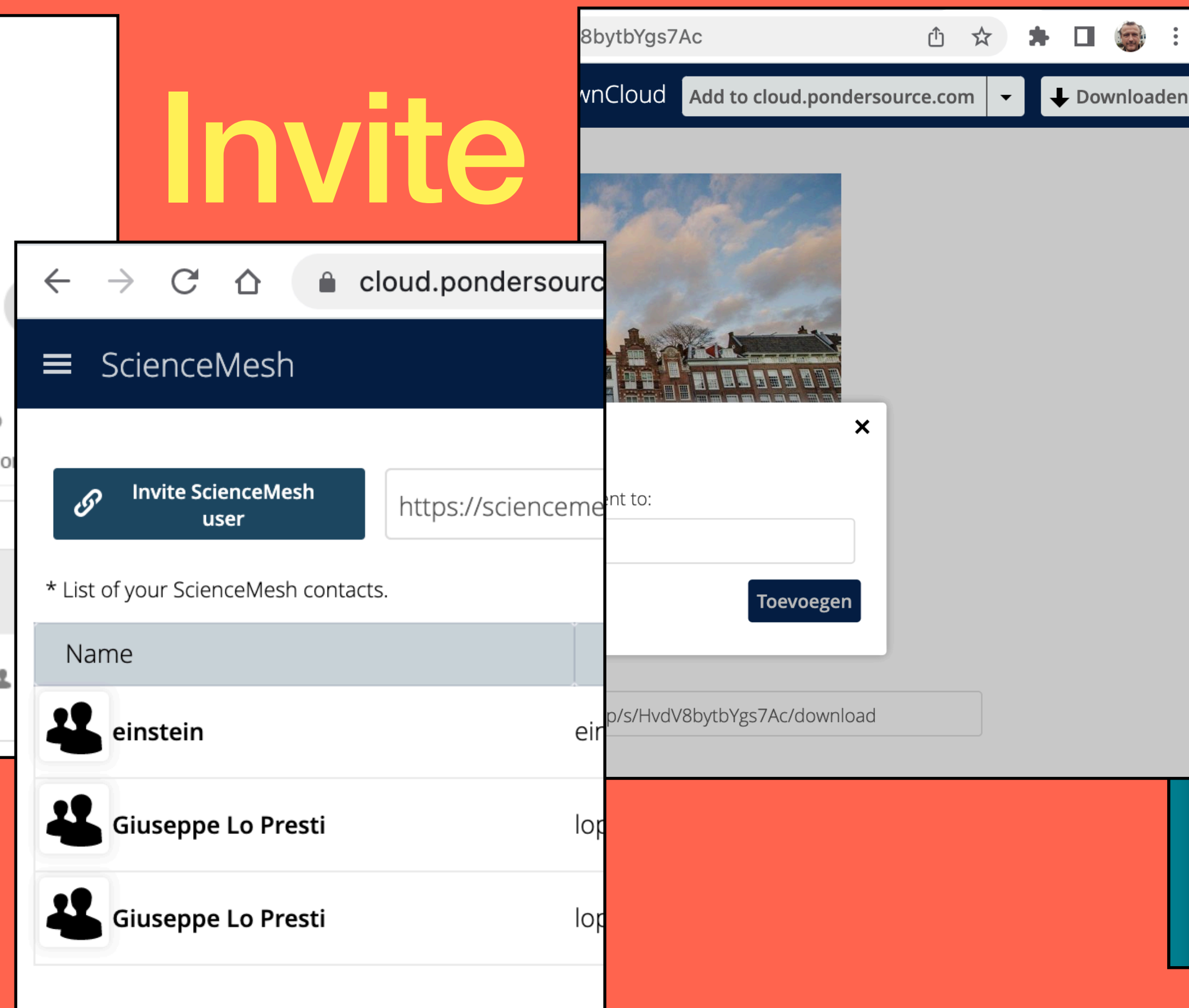
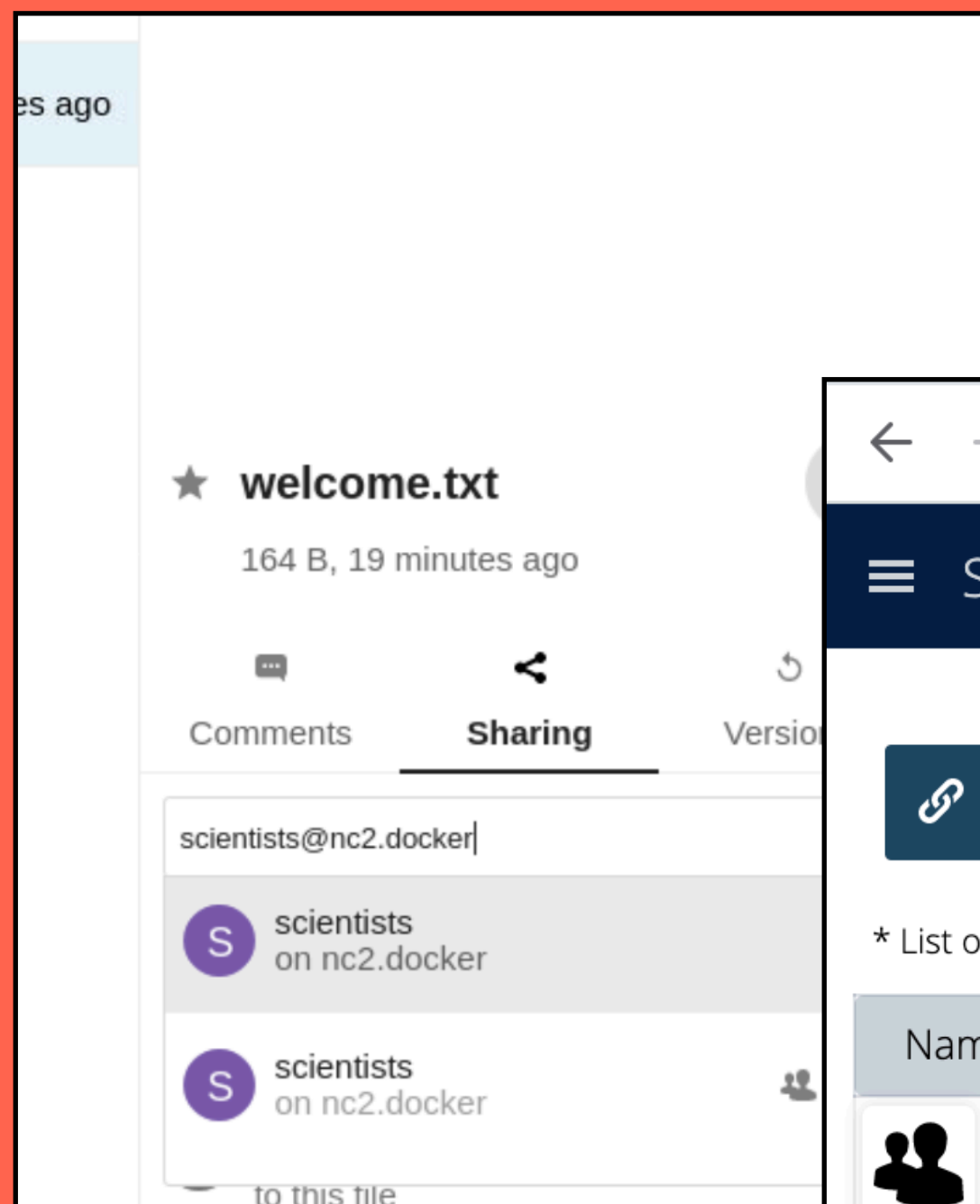
Share-With

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.

Copyright Notice

Copyright (c) 2024 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.

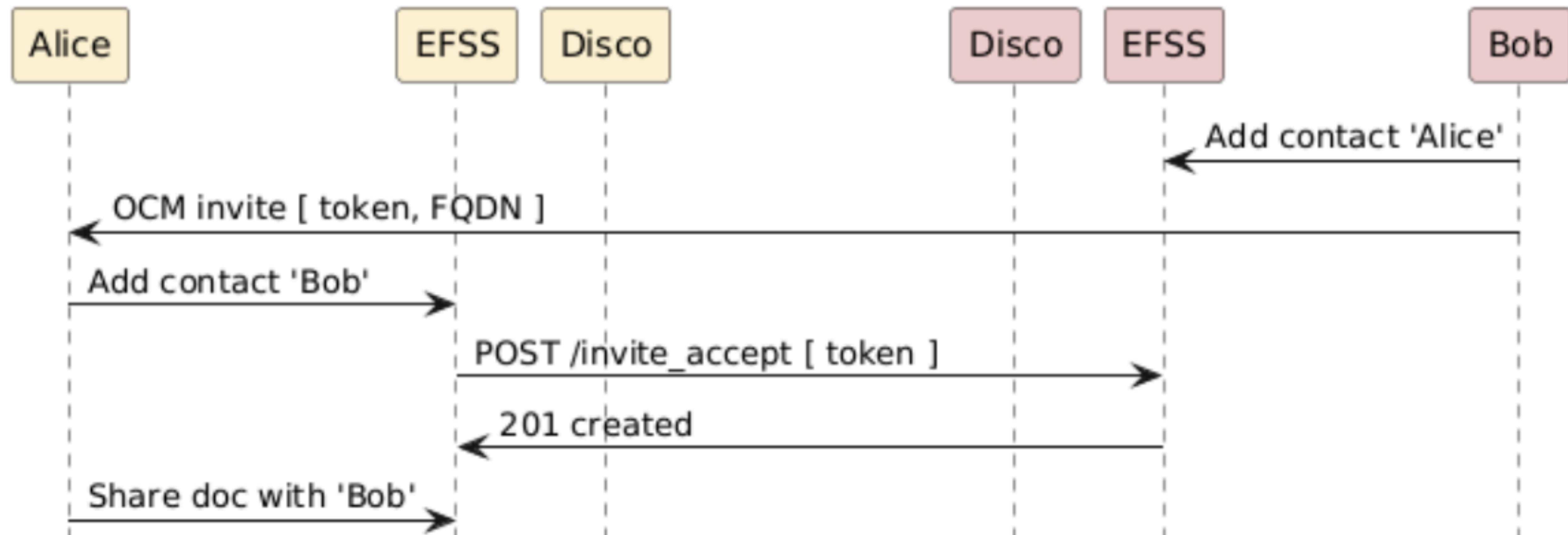
1. Terms

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

- 1. Terms
- 2. General Flow
- 3. Establishing Contact
 - 3.1. Direct Entry
 - 3.2. Address books
 - 3.3. Public Link Flow
 - 3.4. Public Invite Flow
 - 3.5. Invite Flow
 - 3.5.1. Steps
 - 3.5.2. Invite Acceptance Request Details
 - 3.5.3. Invite Acceptance Response Details
 - 3.5.4. Addition into address books
 - 3.5.5. Security Advantages
- 4. OCM API Discovery
 - 4.1. Process
 - 4.2. Fields
- 5. Share Creation Notification
 - 5.1. Fields
 - 5.2. Decision to Discard
- 6. Receiving Party Notification
- 7. Share Acceptance Notification
 - 7.1. Fields
 - 7.1.1. Receiving Party Notification
- 8. Resource Access
- 9. Share Deletion
- 10. Share Updating
- 11. Resharing
- 12. Appendix A: Multi Factor Authentication
- 13. Appendix B: Request Signing
 - 13.1. How to generate the Signature for outgoing request
 - 13.1.1. How to confirm Signature on incoming request
 - 13.2. Validating the payload
- Authors' Addresses

Invites help servers trust each other



Caps Disco

CAPS
DISCO?



Caps Disco

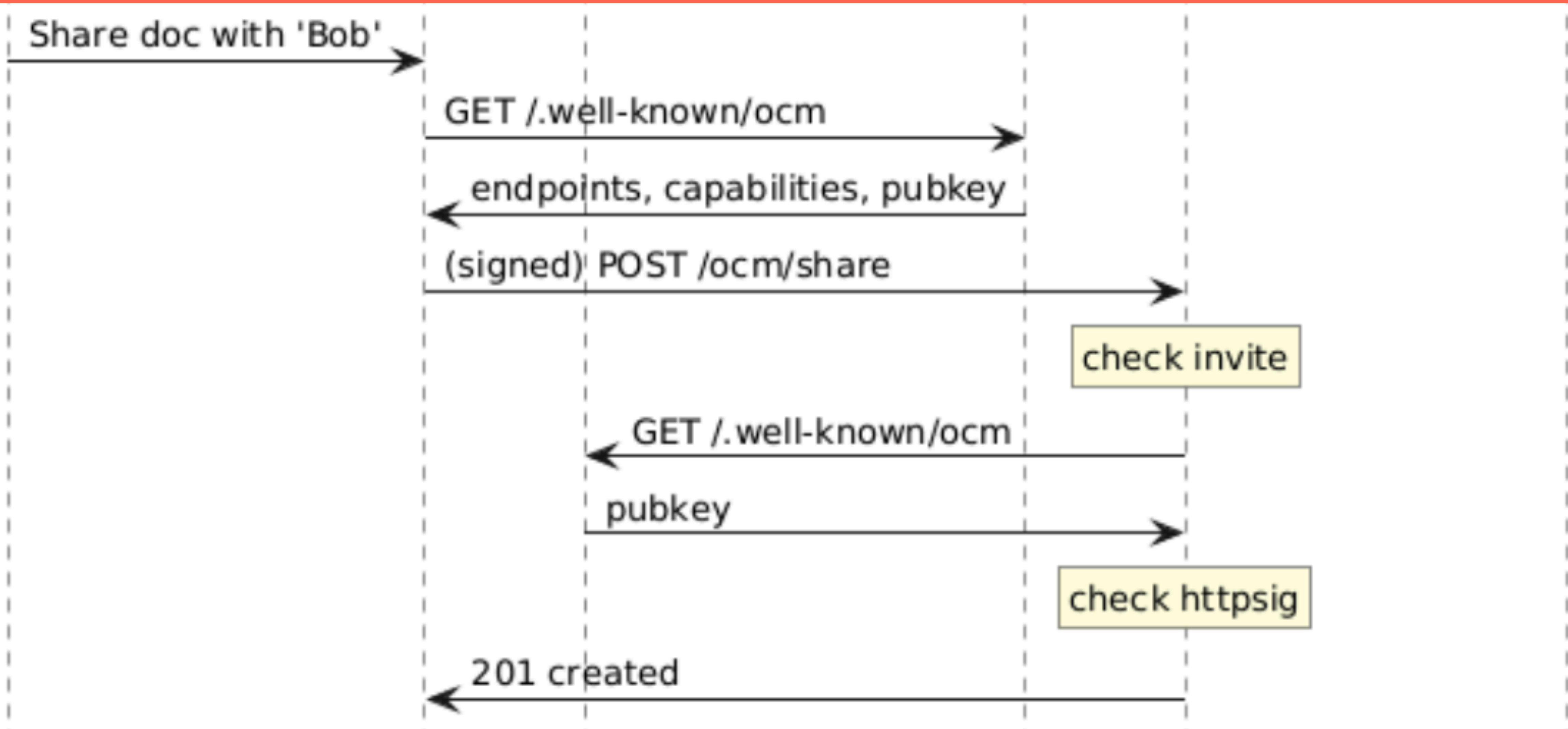
Share doc with 'Bob'

```
sequenceDiagram
    participant A
    participant B
    participant C
    A->>B: Share doc with 'Bob'
    B->>C: GET /.well-known/ocm
    C-->>B: endpoints, capabilities, pubkey
```

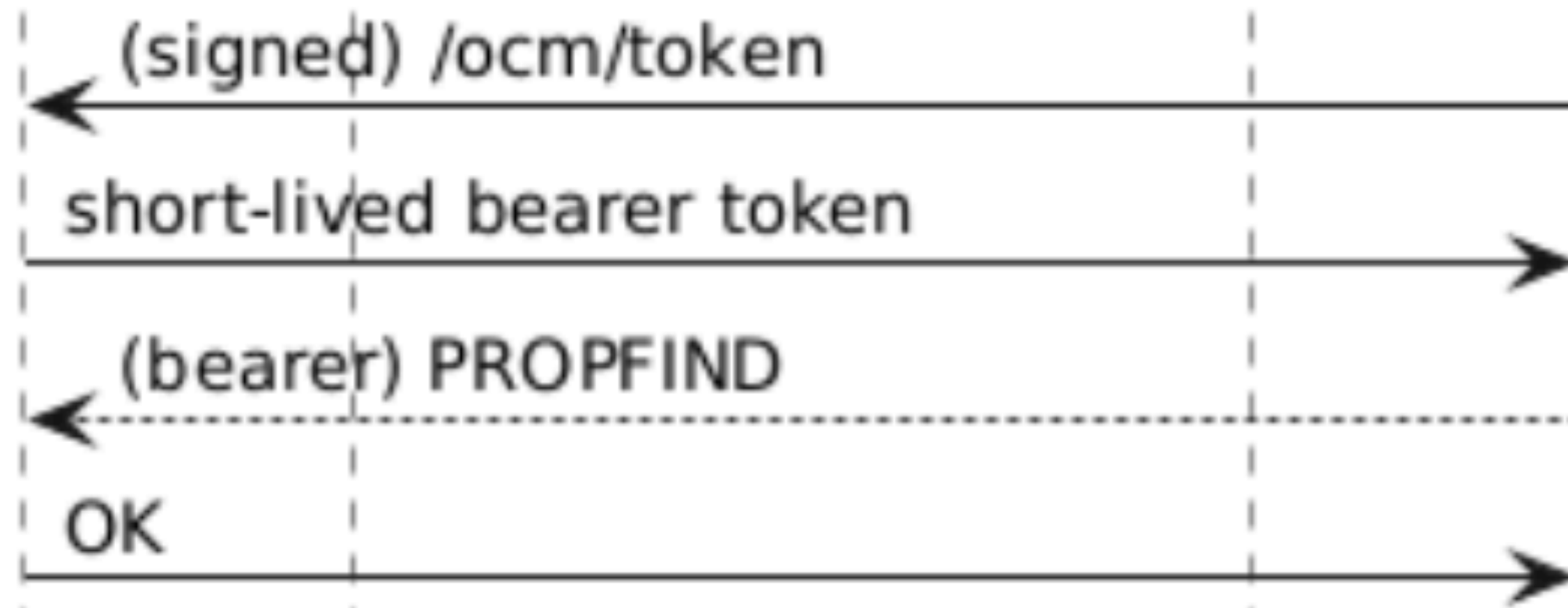
GET /.well-known/ocm

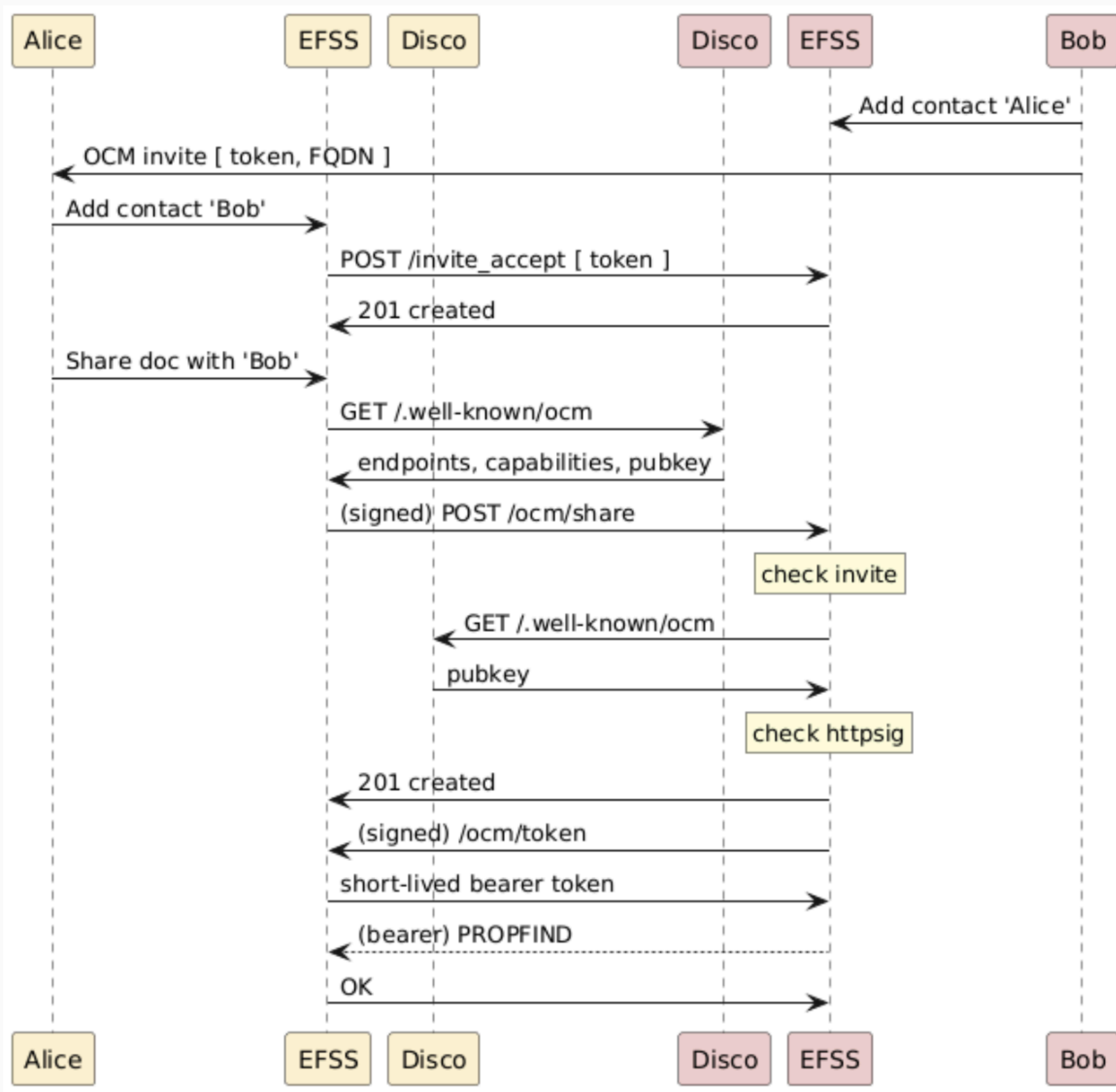
endpoints, capabilities, pubkey

Share Creation Notification



Exchange Code for Token





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