Trusted servers and MFA with OCM

CS32024

Micke Nordin
SUNET

OPENCLOUDMESH

SUNET

Background

Users want to know with whom they share data. MFA is about raising credence in identity, we can use that.

How do we implement MFA across federated EFSS?

We need two things: trusted peers and ability to communicate MFA status between them.

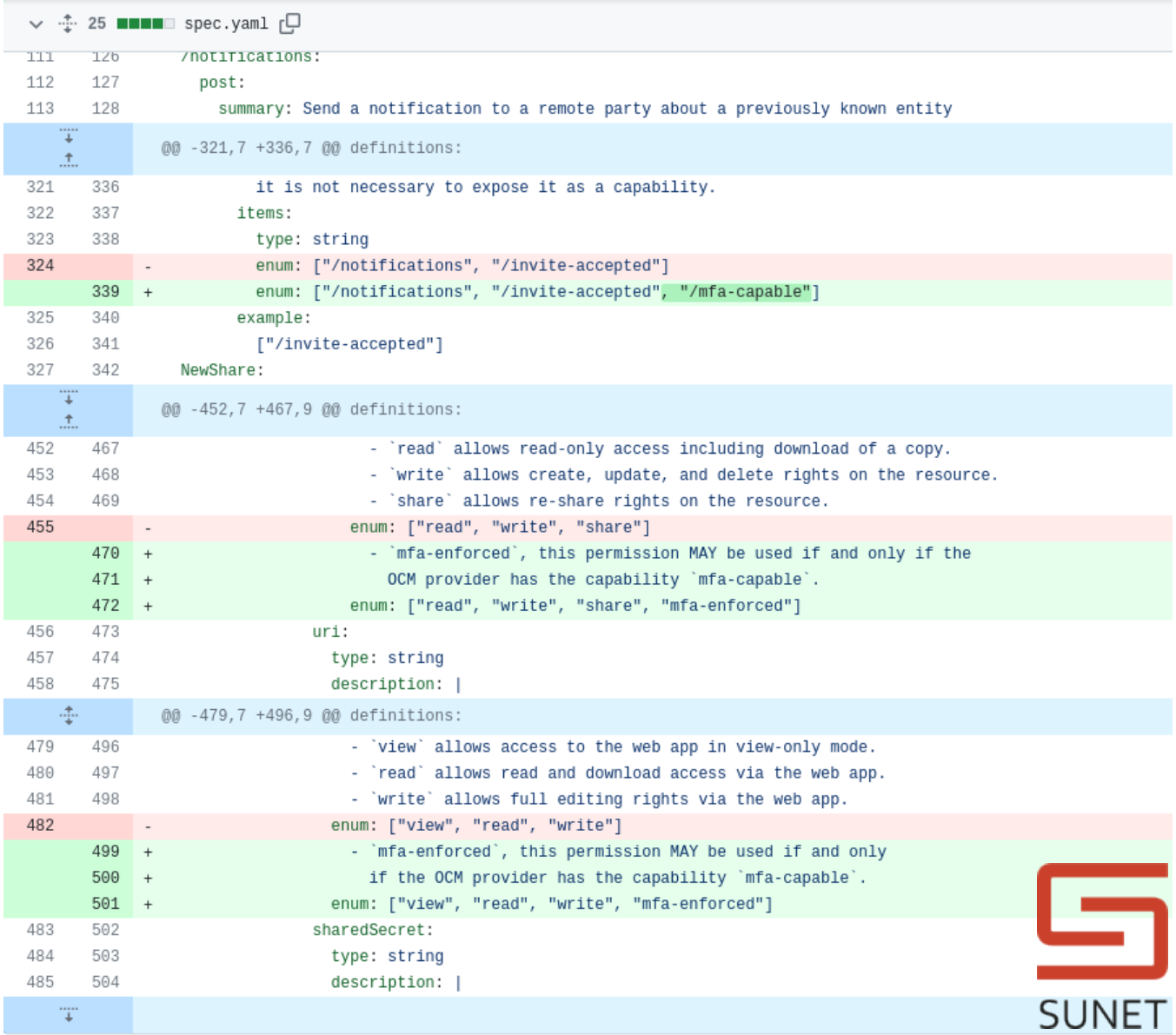
SUNET

MFA in OCM

Establishing trust is out of scope.

When you have trust you can use OCM to signal capabilities for sharing flows.

Signaling capabilites will probably land in OCM v1.2.0



25 spec.yaml

```
111  126     /notifications:
112  127       post:
113  128         summary: Send a notification to a remote party about a previously known entity
                 @@ -321,7 +336,7 @@ definitions:
321  336             it is not necessary to expose it as a capability.
322  337           items:
323  338             type: string
324       -         enum: ["/notifications", "/invite-accepted"]
     339  +         enum: ["/notifications", "/invite-accepted", "/mfa-capable"]
325  340           example:
326  341             ["/invite-accepted"]
327  342     NewShare:
                 @@ -452,7 +467,9 @@ definitions:
452  467                       - `read` allows read-only access including download of a copy.
453  468                       - `write` allows create, update, and delete rights on the resource.
454  469                       - `share` allows re-share rights on the resource.
455       -                 enum: ["read", "write", "share"]
     470  +                   - `mfa-enforced`, this permission MAY be used if and only if the
     471  +                     OCM provider has the capability `mfa-capable`.
     472  +                 enum: ["read", "write", "share", "mfa-enforced"]
456  473               uri:
457  474                 type: string
458  475                 description: |
                 @@ -479,7 +496,9 @@ definitions:
479  496                       - `view` allows access to the web app in view-only mode.
480  497                       - `read` allows read and download access via the web app.
481  498                       - `write` allows full editing rights via the web app.
482       -                 enum: ["view", "read", "write"]
     499  +                   - `mfa-enforced`, this permission MAY be used if and only
     500  +                     if the OCM provider has the capability `mfa-capable`.
     501  +                 enum: ["view", "read", "write", "mfa-enforced"]
483  502               sharedSecret:
484  503                 type: string
485  504                 description: |
```

SUNET