Enabling lightweight and federated accounts access in CERNBox

Ishank Arora
EOS Workshop ‘22

Lightweight and federated accounts

Why?

- Collaboration at CERN happens across boundaries and institutes
  - Need to share data with such collaborators
- Users currently use public links as a workaround to share data
  - Not scalable
  - No traceability

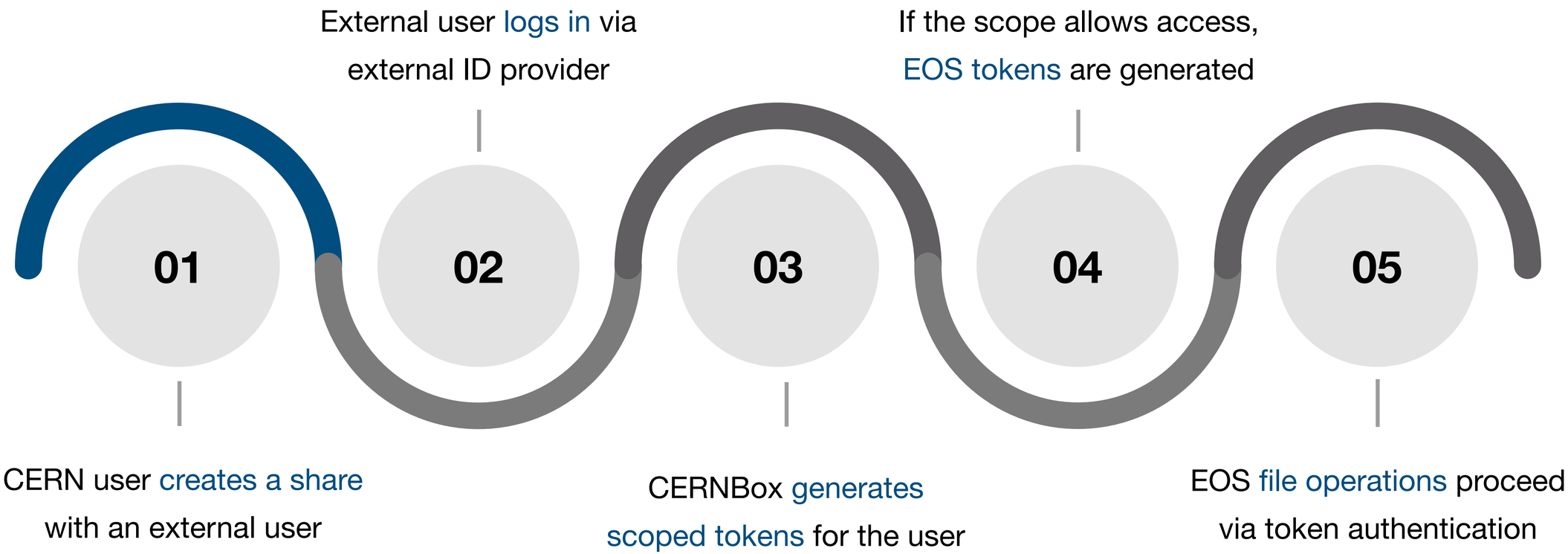
Lightweight access

Behind the scenes

- **RBAC mechanisms**
  - Restricted access scopes
  - Handling expansions
  - Configurable policies
- **EOS Tokens** for Authorisation
  - Access delegation
  - Token Revocation

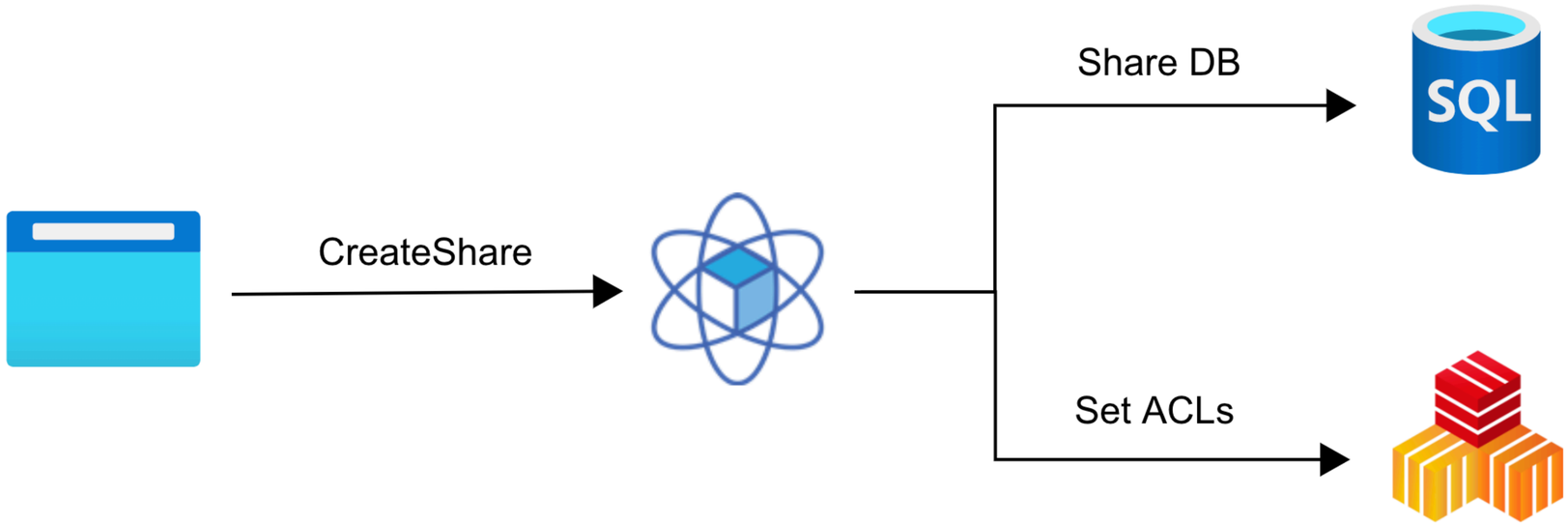
Lightweight access

Workflow



Lightweight access

Share creation for normal users



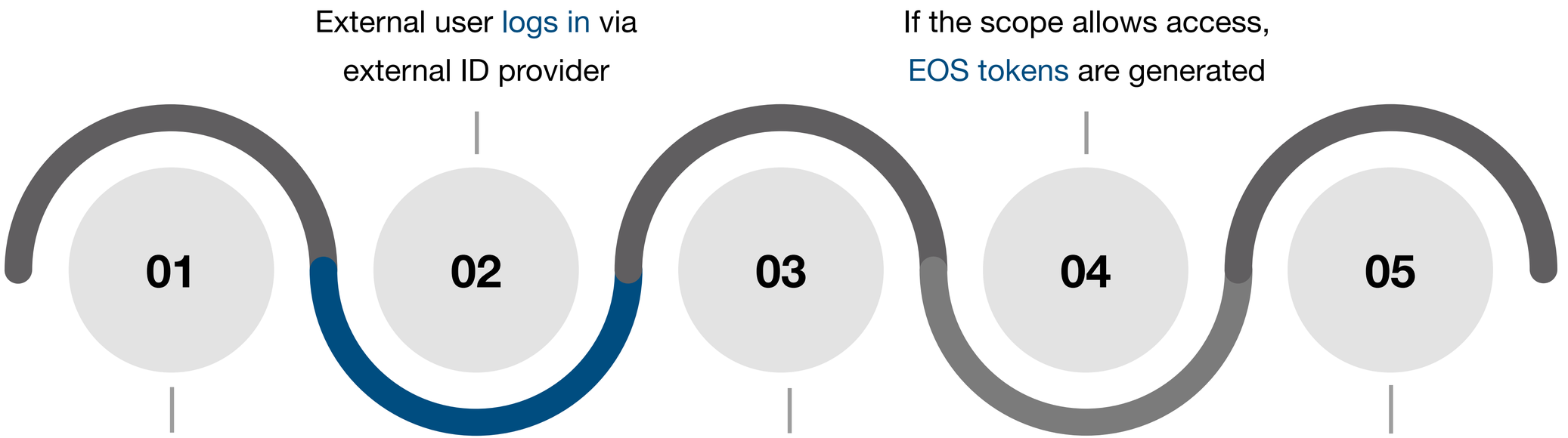
Lightweight access

ACLs

- ACLs look like
  - **`userid`**`=permissions`
- EOS takes care of access control if **`userid`** exists in its linux namespace
  - For lightweight accounts, it does not.
  - Access control to be implemented in our storage microservice

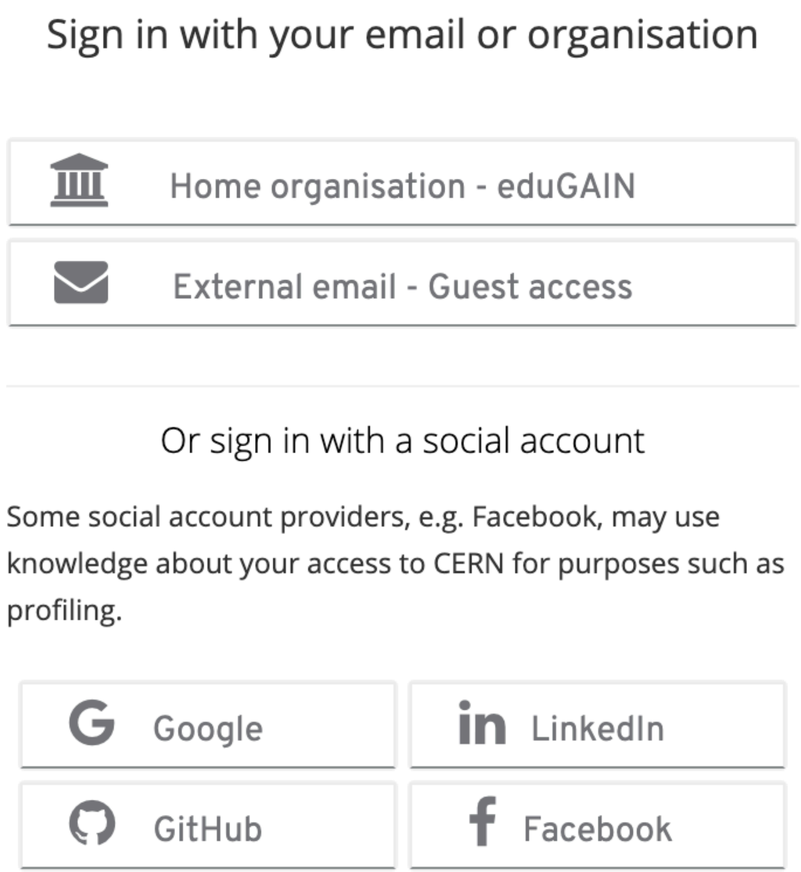
Lightweight access

Workflow

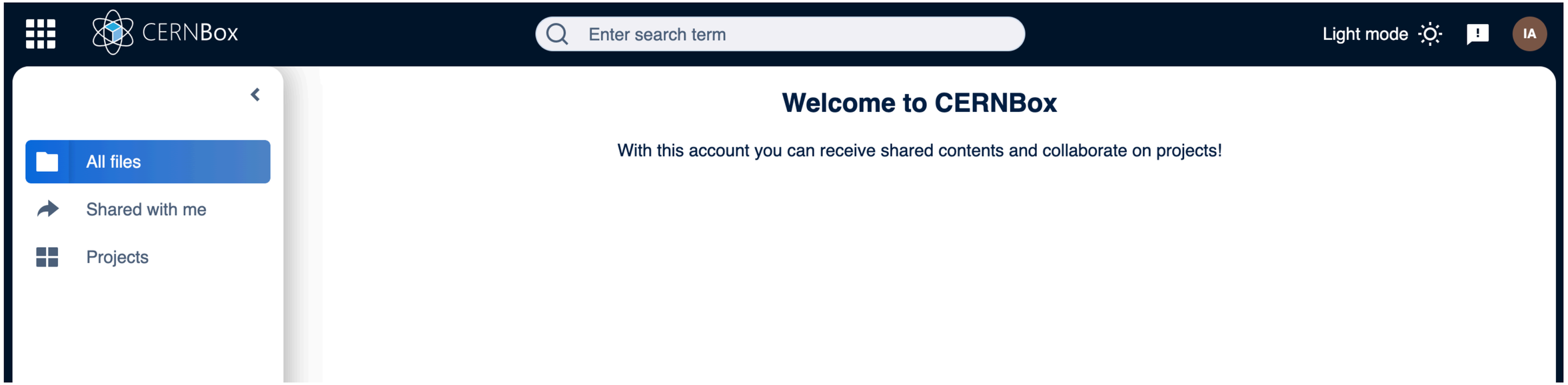


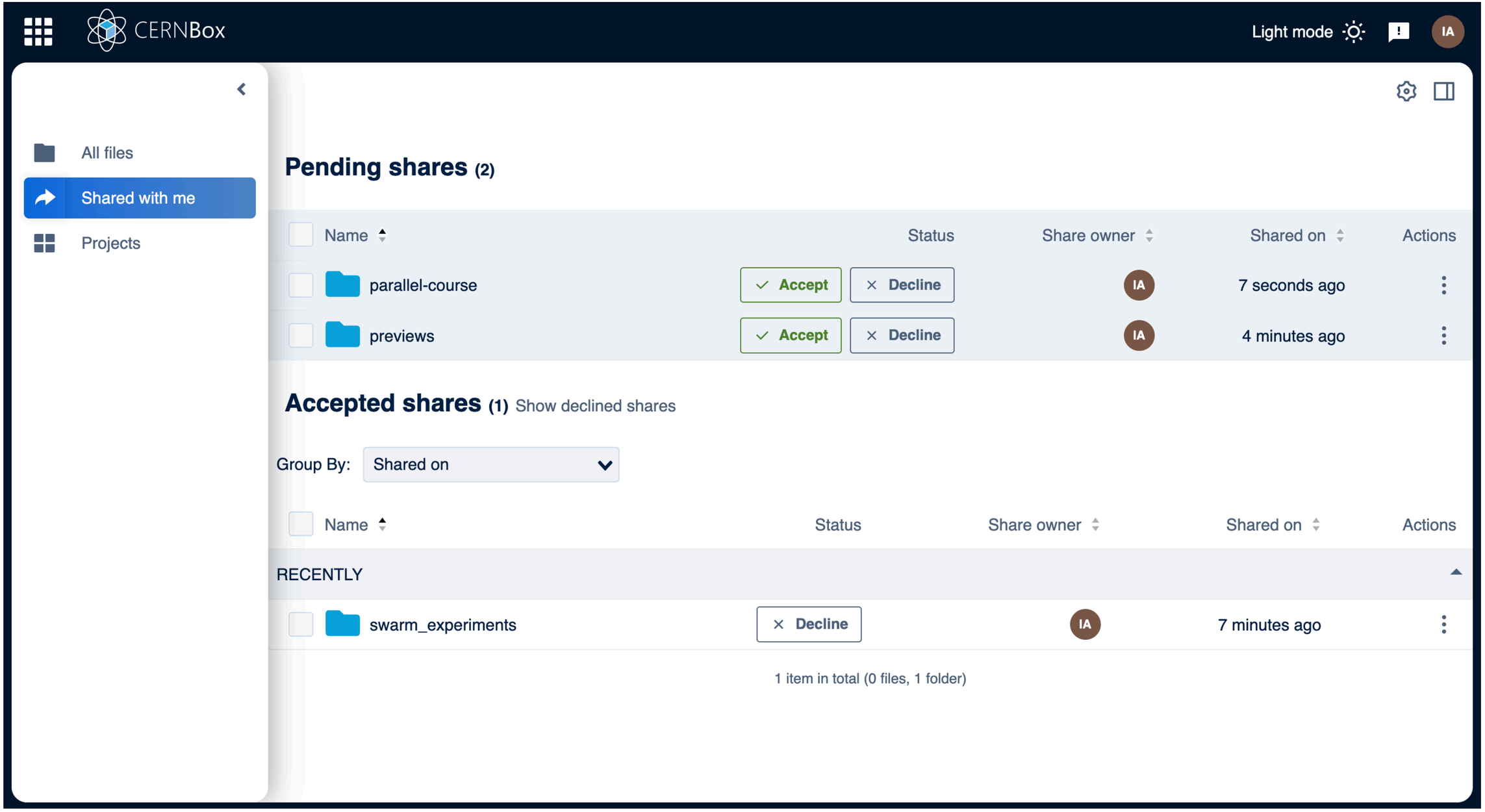
Lightweight access

Keycloak Access



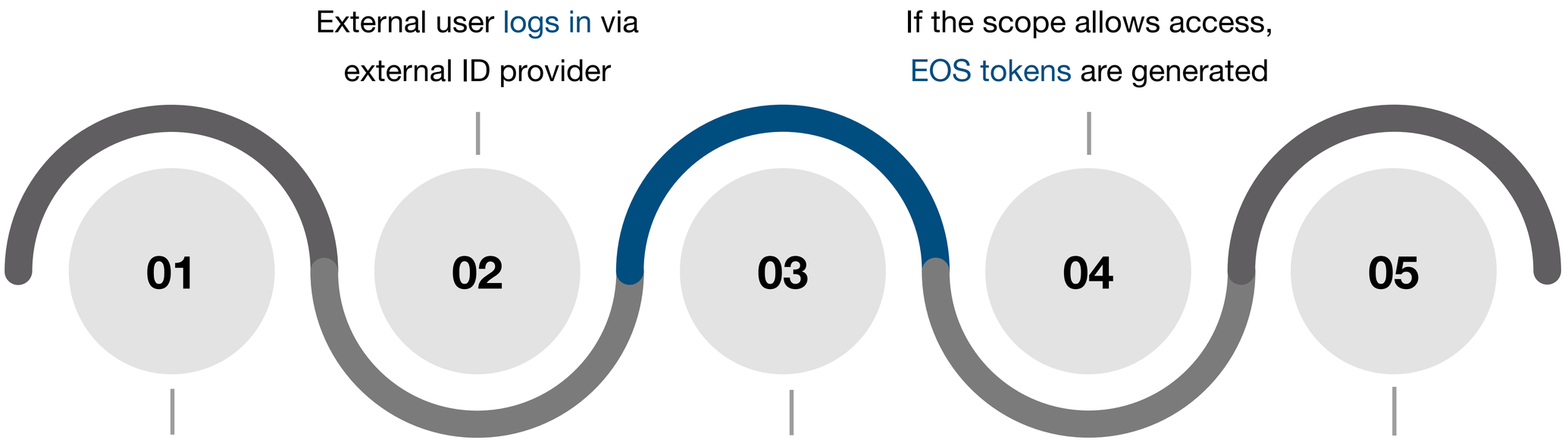
- alice@**gmail.com**
- 109847@**github**
- bob@**xyzuniversity.edu**


CERNBox
Enter search term
Light mode
IA
All files
Shared with me
Projects
Welcome to CERNBox
With this account you can receive shared contents and collaborate on projects!


CERNBox
Light mode
IA
All files
Shared with me
Projects
Pending shares (2)
Name
Status
Share owner
Shared on
Actions
parallel-course
Accept
Decline
IA
7 seconds ago
previews
Accept
Decline
IA
4 minutes ago
Accepted shares (1) Show declined shares
Group By:
Shared on
Name
Status
Share owner
Shared on
Actions
RECENTLY
swarm_experiments
Decline
IA
7 minutes ago
1 item in total (0 files, 1 folder)

Lightweight access

Workflow



Lightweight access

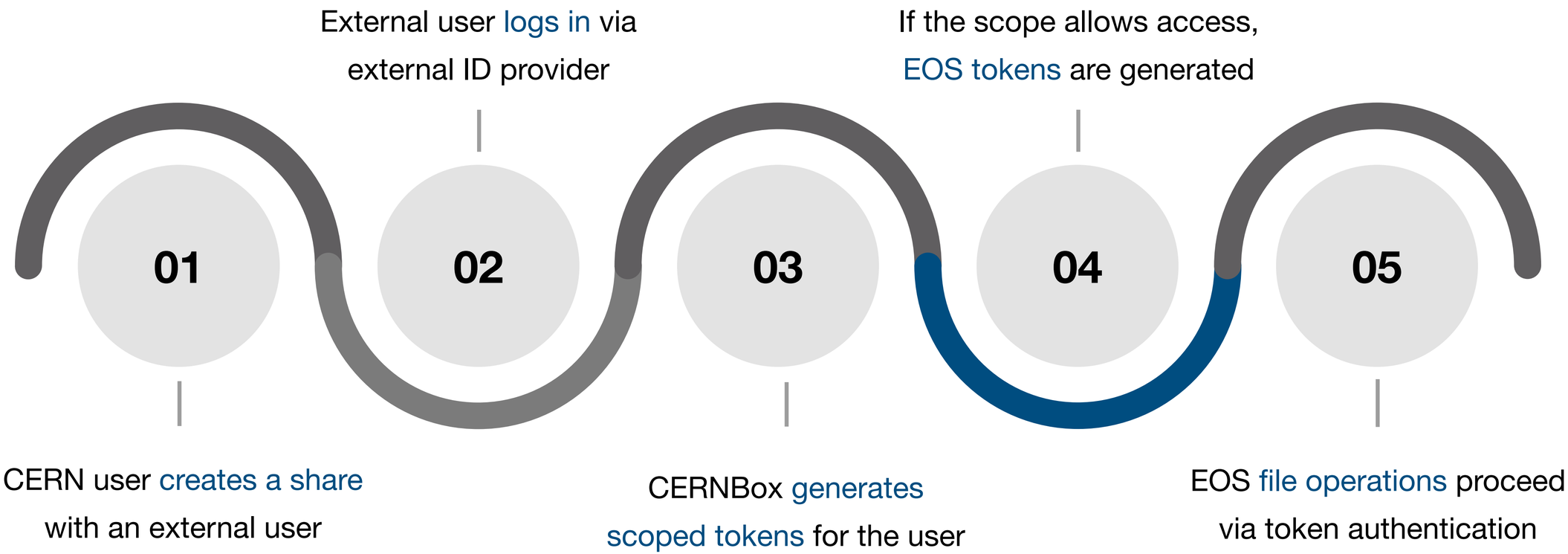
Scoped tokens

```
{
  "aud": "reva",
  "iss": "https://auth.cern.ch",
  "user": {
    "id": {
      "opaque_id": "guest:ishank011@gmail.com",
      "type": "lightweight"
    },
    "username": "guest:ishank011@gmail.com",
    "mail": "ishank011@gmail.com",
    "display_name": "Guest User"
  },
  "scope": [
    "lightweight"
  ]
}
```

```
{
  "scopes": {
    "lightweight": {
      "http": [
        "/apps/files_sharing/api/v1/shares",
        "/cloud/capabilities",
        "/cloud/user",
        "/webdav",
        "/dav/files",
        "/app",
        "/data"
      ],
      "grpc": [
        "ListReceivedShares",
        "scope:share",
        "scope:resourceInfo"
      ]
    }
  }
}
```

Lightweight access

Workflow



Lightweight access

Scope Verification

- **Scenario 1: User lists received shares**
  - GET `/apps/file_sharing/api/v1/shares?received=true`
    - Calls `ListReceivedShares`
    - Response:
      - `/eos/user/i/ishank/myfolder (rw)`
      - `/eos/user/a/Alice/results (r)`
      - `/eos/project/s/simulations/myfolder (rw)`


```
{
  "scopes": {
    "lightweight": {
      "http": [
        "/apps/files_sharing/api/v1/shares",
        "/cloud/capabilities",
        "/cloud/user",
        "/webdav",
        "/dav/files",
        "/app",
        "/data"
      ],
      "grpc": [
        "ListReceivedShares",
        "scope:share",
        "scope:resourceInfo"
      ]
    }
  }
}
```

Lightweight access

Scope Expansion

- **Scenario 2: Scope expansion**
  - `/eos/user/i/ishank/myfolder`
  - `/eos/user/a/alice/results`
  - `/eos/project/s/simulations/myfolder`

```
{
  "scopes": {
     "lightweight": {
        "http": [
           "..."
        ],
        "grpc": [
           "ListReceivedShares",
           "scope:share",
           {
           → "scope:resourceInfo": [
                 "/eos/user/i/ishank/myfolder",(rw)
                 "/eos/user/a/alice/results",(r)
                 "/eos/project/s/simulations/myfolder"(rw)
              ]
           }
        ]
     }
  }
}
```

Lightweight access

Scope Verification

- **Scenario 3: User lists a folder**
  - PROPFIND `/eos/user/i/ishank/myfolder`
    - Scope verified!
    - Response:
      - `textfile.txt -> eos-01:789`
      - `document.docx -> eos-01:790`
      - `present.pptx -> eos-02:654`
    - Expand scope again!

```
{
  "scopes": {
     "lightweight": {
        "http": [
           "..."
        ],
        "grpc": [
           "ListReceivedShares",
           "scope:share",
           {
              "scope:resourceInfo": [
                 "/eos/user/i/ishank/myfolder",(rw)
                 "/eos/user/a/alice/results",(r)
                 "/eos/project/s/simulations/myfolder"(rw)
              ]
           }
        ]
     }
  }
}
```

Lightweight access

Scope Expansion - II

```
{
  "scopes": {
     "lightweight": {
        "http": [
           "..."
        ],
        "grpc": [
           "...",
           {
              "scope:resourceInfo": [
                 "/eos/user/i/ishank/myfolder",(rw)
                 "/eos/user/a/alice/results",(r)
                 "/eos/project/s/simulations/myfolder",(rw)
                 "eos-01:789",(rw)
                 "eos-01:790",(rw)
                 "eos-02:654" (rw)
              ]
           }
        ]
     }
  }
}
```

Lightweight access

Scope Verification

- **Scenario 4: User accesses a file**
  - GET `/eos/user/i/ishank/myfolder/textfile.txt`
    - Scope verified!
  - POST `/app/open?file=eos-01:790`
    - Scope verified!

Lightweight access

Scope Verification

- **Scenario 5: User accesses a file not in scope**
  - GET `/eos/user/b/bob/videos/skiing.mov`
    - Call `ListReceivedShares`
    - Response:
      - ...
      - `/eos/user/b/bob/videos`
    - Scope verified!
    - Expand scope again!

```
{
  "scopes": {
    "lightweight": {
      "http": [
        "..."
      ],
      "grpc": [
        "...",
        {
          "scope:resourceInfo": [
            "/eos/user/i/ishank/myfolder",(rw)
            "/eos/user/a/alice/results",(r)
            "/eos/project/s/simulations/myfolder",(rw)
            "eos-01:789",(rw)
            "eos-01:790",(rw)
            "eos-02:654"(rw)
          ]
        }
      ]
    }
  }
}
```

Lightweight access

Scope Verification

- **Scenario 6: User accesses a file not in scope**
  - GET `/app/open?file=eos-01:742`
    - GetPathAsRoot `eos-01:742`
      - Path: `/eos/user/a/Alice/results/latest.ipynb`
    - Scope verified!
    - Expand scope again!

```
{
  "scopes": {
    "lightweight": {
      "http": [
        "..."
      ],
      "grpc": [
        "...",
        {
          "scope:resourceInfo": [
            "/eos/user/i/ishank/myfolder",(rw)
            "/eos/user/a/alice/results",(r)
            "/eos/project/s/simulations/myfolder",(rw)
            "eos-01:789",(rw)
            "eos-01:790",(rw)
            "eos-02:654",(rw)
            "/eos/user/b/bob/videos"(r)
          ]
        }
      ]
    }
  }
}
```

Lightweight access

Scope Verification

- **Scenario 7: Share creator removes share**
  - Start background routine to shrink scope

```
{
  "scopes": {
     "lightweight": {
        "http": [
           "..."
        ],
        "grpc": [
           "...",
           {
              "scope:resourceInfo": [
                 "/eos/user/i/ishank/myfolder",(rw)
              ✕ "/eos/user/a/alice/results",(r)
                 "/eos/project/s/simulations/myfolder",(rw)
                 "eos-01:789",(rw)
                 "eos-01:790",(rw)
                 "eos-02:654",(rw)
                 "/eos/user/b/bob/videos"(r)
              ]
           }
        ]
     }
  }
}
```

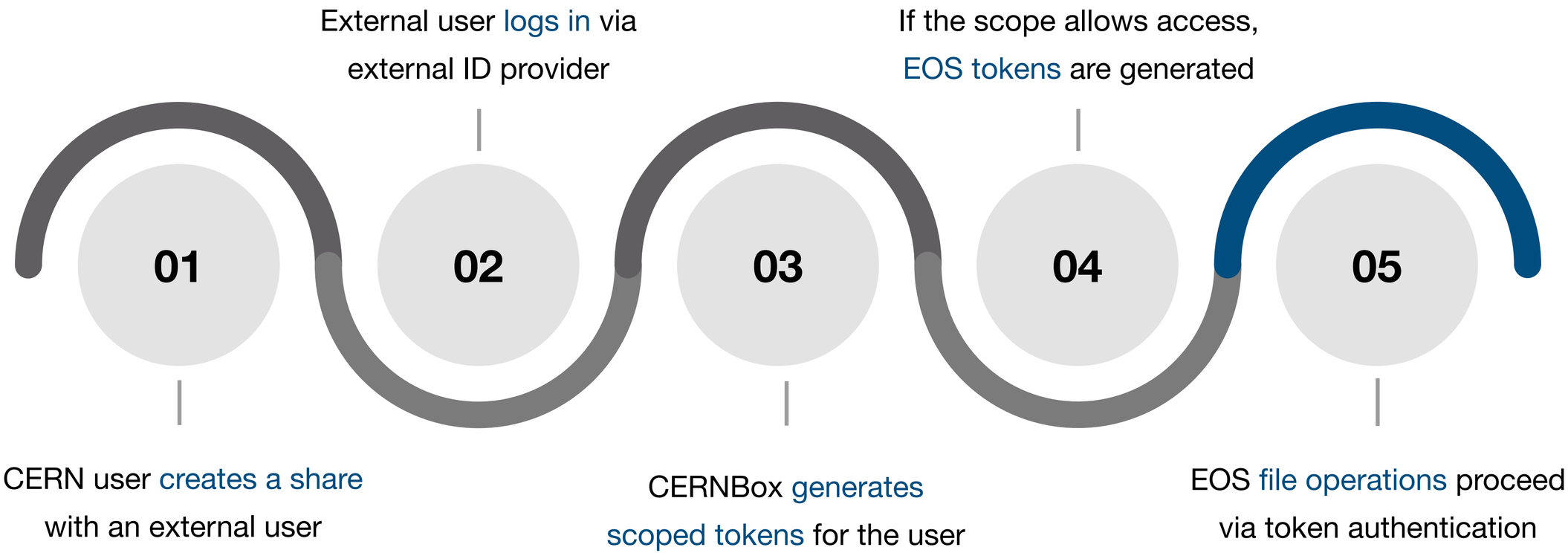
Lightweight access

Token Generation

```
$ eos token

    --permission rwx

    --path /eos/myfile

    --expires $LATER

zteos64:MDAwMDAwNzR4nONS4WIuKq8Q-Dlz-
ltWI3H91Pxi~cSsAv2S~OzUPP2SeAgtpMAY7f1e31Ts-od-
rgcLZ~a2~bhwcZO9cracyhm1b3c6jpRIEWWOws71Ox6xAABeTC8I
```

Lightweight access

Workflow



Lightweight access

Authentication via Tokens

```
$ EOSAUTHZ=$TOKEN eos stat /eos/myfile

$ xrdcp "root://myeos//eos/myfile?authz=$TOKEN" /tmp/
```

Thoughts

- Reinventing ACLs?
  - The mechanism is not restricted to files
- Can set custom sys attributes in EOS and implement basic access control?
  - `sys.cernbox.lwshare = "user:109847@github = rx,`

    `user:guest:alice@gmail.com = rwx"`
  - The RBAC mechanism was developed for public links
    - Where we impersonate the share owner for EOS access
    - EOS tokens did not exist previously

Thank you!

Questions?

ishank.arora@cern.ch