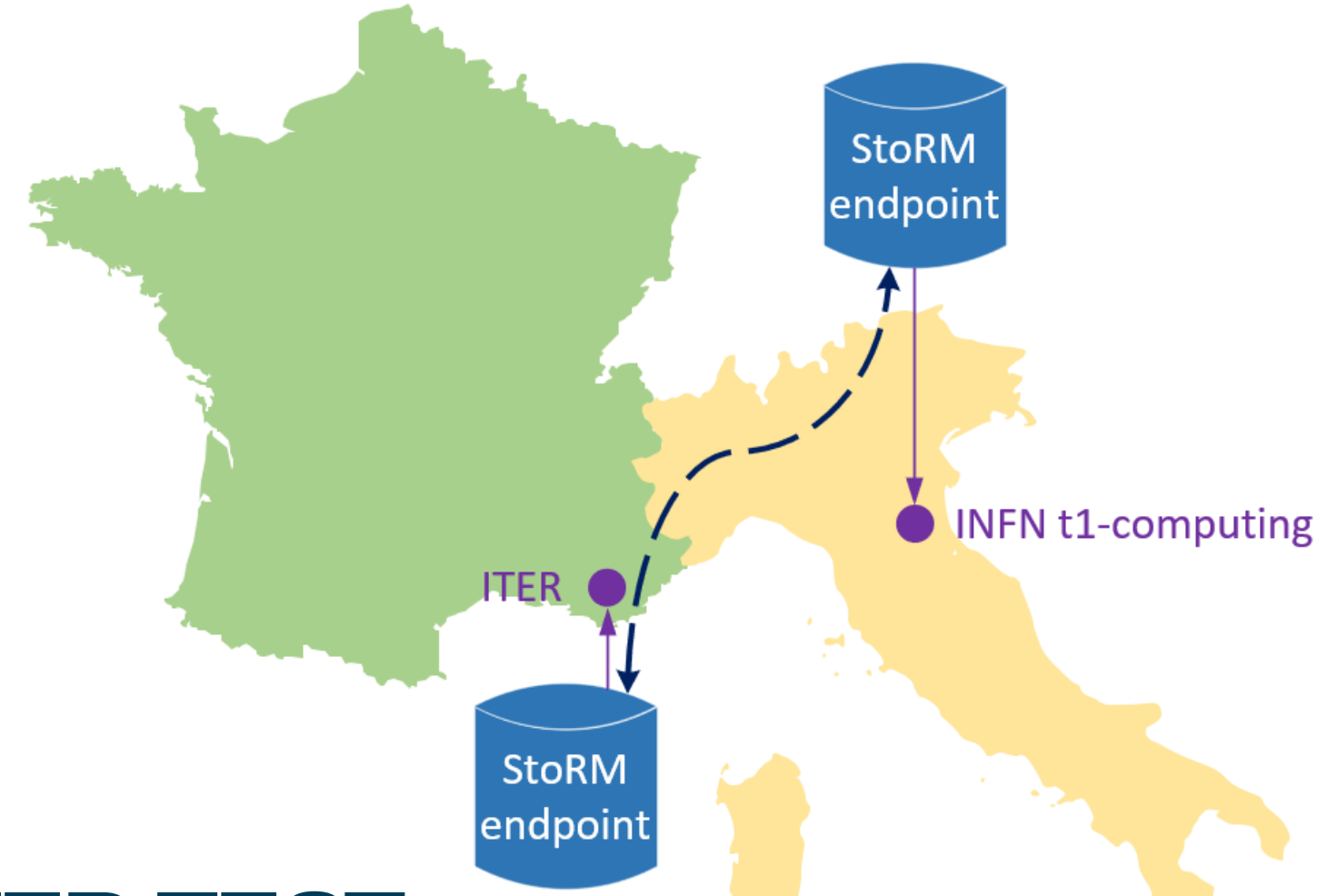


StoRM ITER TEST

ITER-INFM meeting

Lobes Leonid

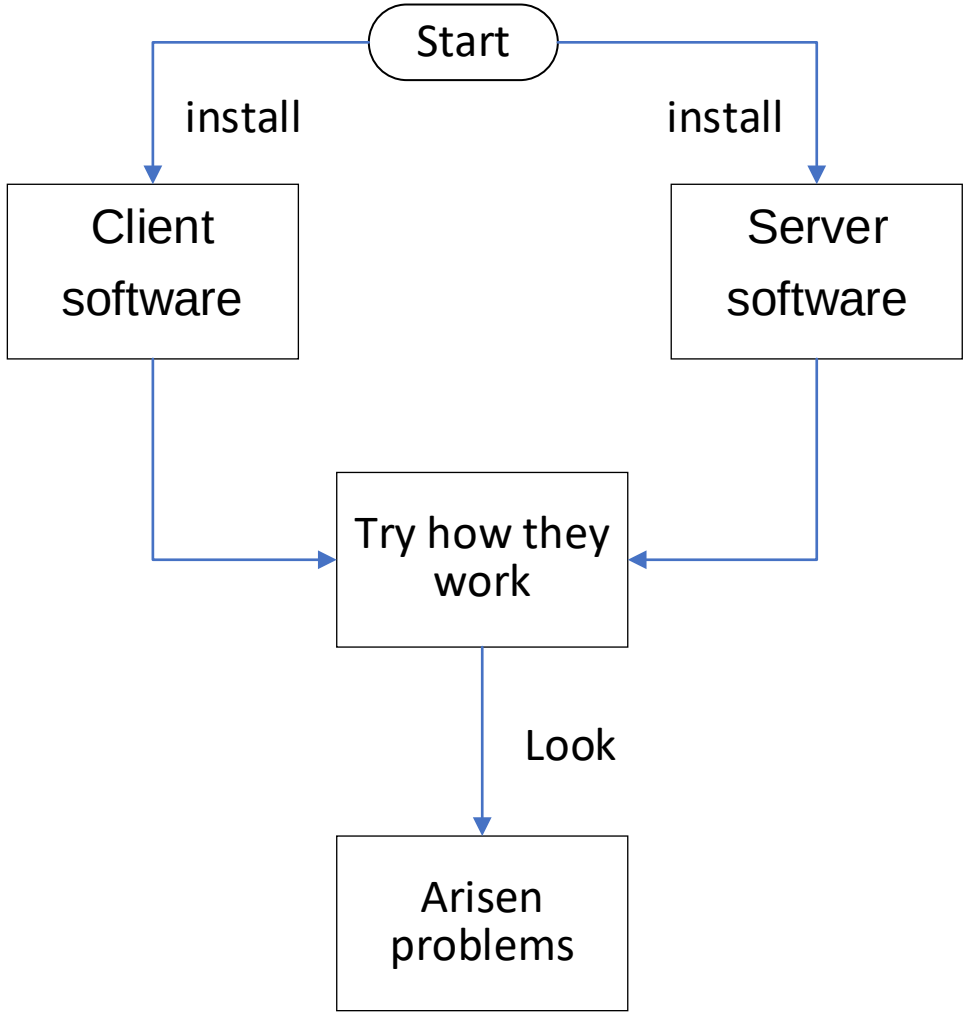
23.07.2024

iter

china eu india japan korea russia usa

Introduction

1. look to the **client** software
2. look to the **server** software
3. try how it works
4. look at the **problems** that have arisen



Client installing. Tested on: Rocky Linux 8 (WSL2) instance on ITER laptop.

https://docs.rockylinux.org/guides/interoperability/import_rocky_to_wsl/

1. update repositories → `dnf update`

2. add epel-release → `dnf install epel-release` then `dnf update`

3. Install oidc agent and gfal2 tools: → `dnf install oidc-agent-cli` then `dnf install gfal2-all gfal2-util-scripts`

4. install python gfal2 utilities, for that `powertools` is required. → `dnf config-manager --set-enabled powertools` then `dnf install python3-gfal2 python3-gfal2-util`

5. some additional requirements: → `dnf install jq`

NOTE

It will not work so far. Possibly due to lack of necessary certificates.

IMPORTANT

Now and only now, after all above already installed, the order is important: we need to add several packages from the `umd-release` repository for centos7.
Otherwise there is a lot of conflicts.

Client installing. Tested on: Rocky Linux 8 (WSL2) instance on ITER laptop.

So we'll use **some hack**, install **`ca-policy-egi-core`** from **`umd-release`** repo for **centos7**.

Install downloaded rpm:

```
dnf localinstall /data/yum-priorities/yum-plugin-priorities-1.1.31-54.el7_8.noarch.rpm
```

than install `umd-release` repo and package:

```
dnf install http://repository.egi.eu/sw/production/umd/4/centos7/x86_64/updates/umd-release-4.1.3-1.el7.centos.noarch.rpm
dnf update
dnf install ca-policy-egi-core -y
```

Client using. Tested on: Rocky Linux 8 (WSL2) instance on ITER laptop.

1. You need to be registered in INFM computing
2. Register device:

```
eval `oidc-agent-service use`
oidc-gen -w device

Enter short name for the account to configure: wRocky8
Issuer [https://aai-dev.egi.eu/auth/realms/egi]: https://iam-t1-computing.cloud.cnaf.infn.it/
Scopes or 'max' (space separated) [openid profile offline_access]: max
```

Then follow the instructions to finish registration. That also will ask you to register token in INFM side.

3. Some additional setup from our(client) side:

```
oidc-add "wRocky8"
export BEARER_TOKEN=$(oidc-token "wRocky8")
unset X509_USER_PROXY
```

Usage example in next slide

Client using. Tested on: Rocky Linux 8 (WSL2) instance on ITER laptop.

Here client part is completed. Can be tested like:

```
[root@client-wsl ~]# gfal-copy https://xfer-test.cr.cnaf.infn.it:8443/iter/test local_data.txt test
```

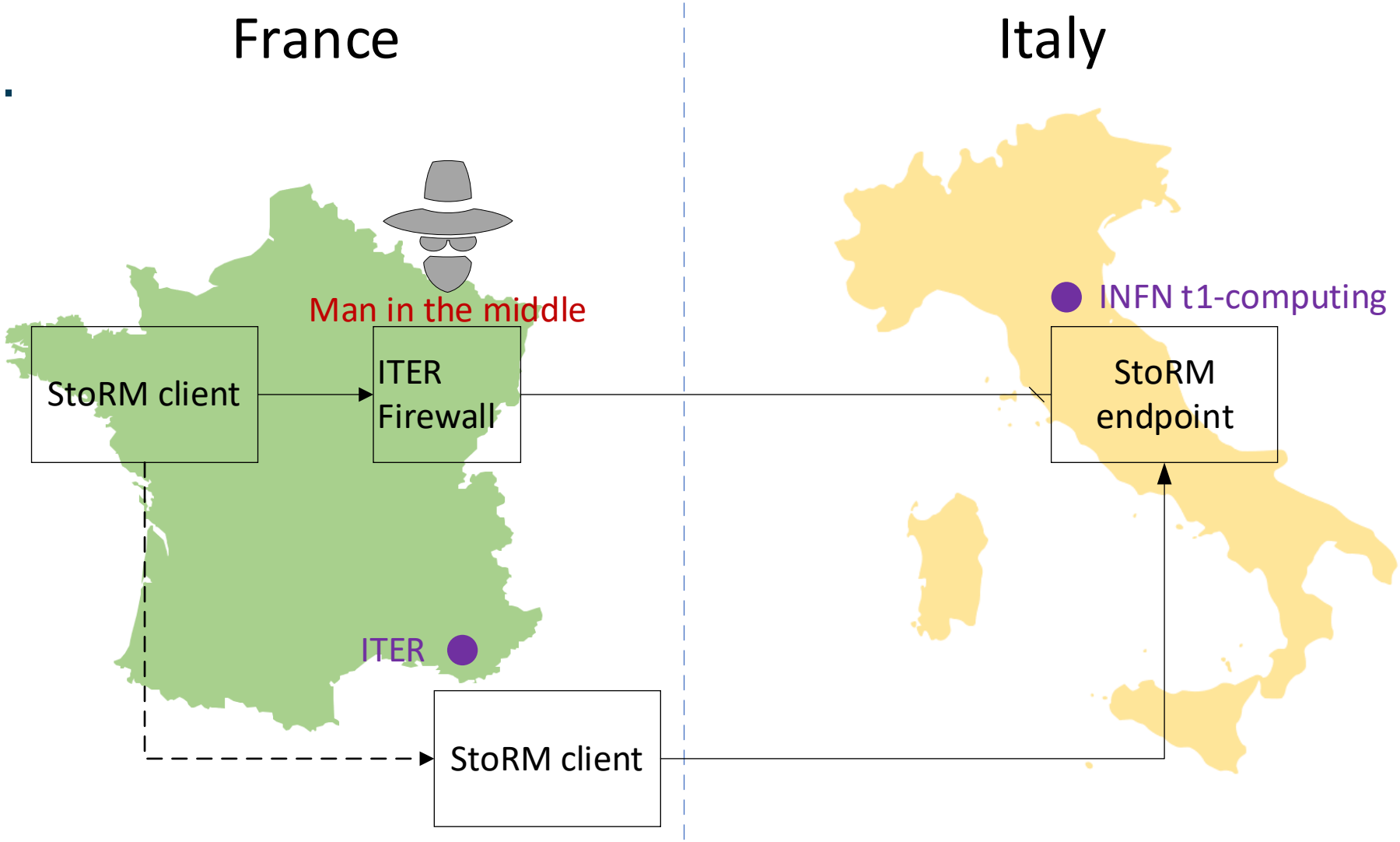
```
[root@client-wsl ~]# gfal-ls davs://xfer-test.cr.cnaf.infn.it:8443/iter
local_data.txt
test
```

Here we get the content of remote directory (which was also created before using the client)

IMPORTANT NOTE

To be able to test with external storage from iter laptop you should be outside ITER.

Client using.



NOTE

Probably iter firewall here act as a classic man in the middle attack, which prevents token validation and authorization

Server installing.

For service installation:

1. Install provided from INFM RPM package for RH8. officially not provided by any CERN repository yet (at the time of writing this presentation)

2. Need to switch Java to version 11 (not by default in RH8)
3. Configure storage
4. Issue and add iter CA certificates (in our case CODAC CA certificates as our test instance inside XPOZ network zone)
5. Configure authentication method.
6. Then if everything setting up correctly service can be runned:

```
● storm-webdav.service - StoRM WebDAV service
   Loaded: loaded (/usr/lib/systemd/system/storm-webdav.service; enabled; vendor preset: disabled)
  Drop-In: /etc/systemd/system/storm-webdav.service.d
           └─filelimit.conf, storm-webdav.conf
   Active: active (running) since Thu 2024-04-18 07:26:01 UTC; 1 months 3 days ago
 Main PID: 225774 (java)
    Tasks: 66 (limit: 204282)
   Memory: 1.0G
   CGroup: /system.slice/storm-webdav.service
           └─225774 /usr/bin/java -Xms1024m -Xmx1024m -Djava.io.tmpdir=/var/lib/storm-webdav/work -Dlogging.config=/etc/storm/webdav/logback.xml -jar /usr/share/java/storm-
webdav/storm-webdav-serv>
```

Server installing summary.

1. ITER not provide any supported authentication methos. Since StoRM is backend, authorization via the web interface is impossible, tokens are required.
   Therefore, our instance now allow any type of actions for anyone

In file: /etc/storm/webdav/config/application.yml

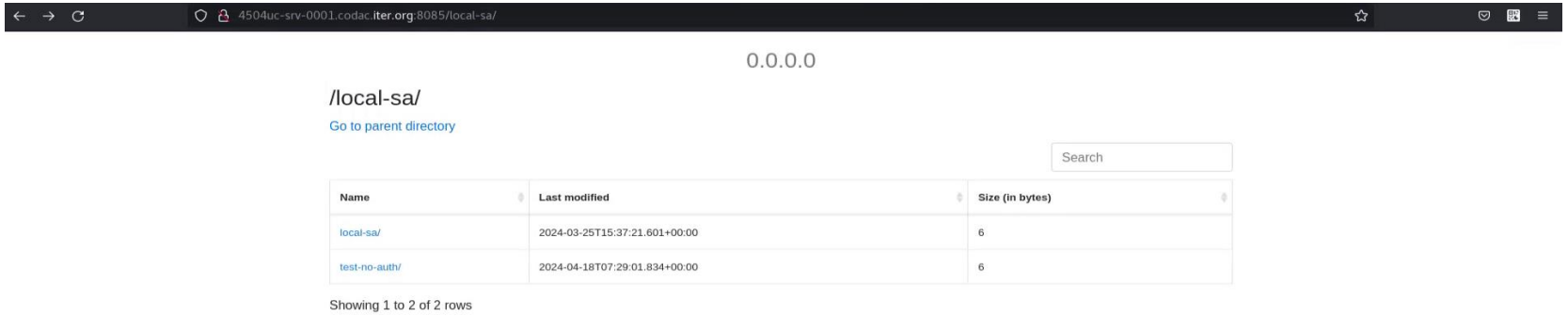
```
storm:
  authz:
    policies:
    - sa: test-sa
      actions:
      - all
      effect: permit
      description: Grant read/write access to any user
      principals:
      - type: anyone
```

And in file: /etc/storm/webdav/sa.d/sa.properties

```
vos=
orgs=
authenticatedReadEnabled=true
anonymousReadEnabled=true
fineGrainedAuthzEnabled=true
```

Server installing summary.

For check installation we can look at it in browser



And for test curl utility can be used (since install client and use it with anonymous access inside CODAC VM not so straight forward)

Example for create folder:

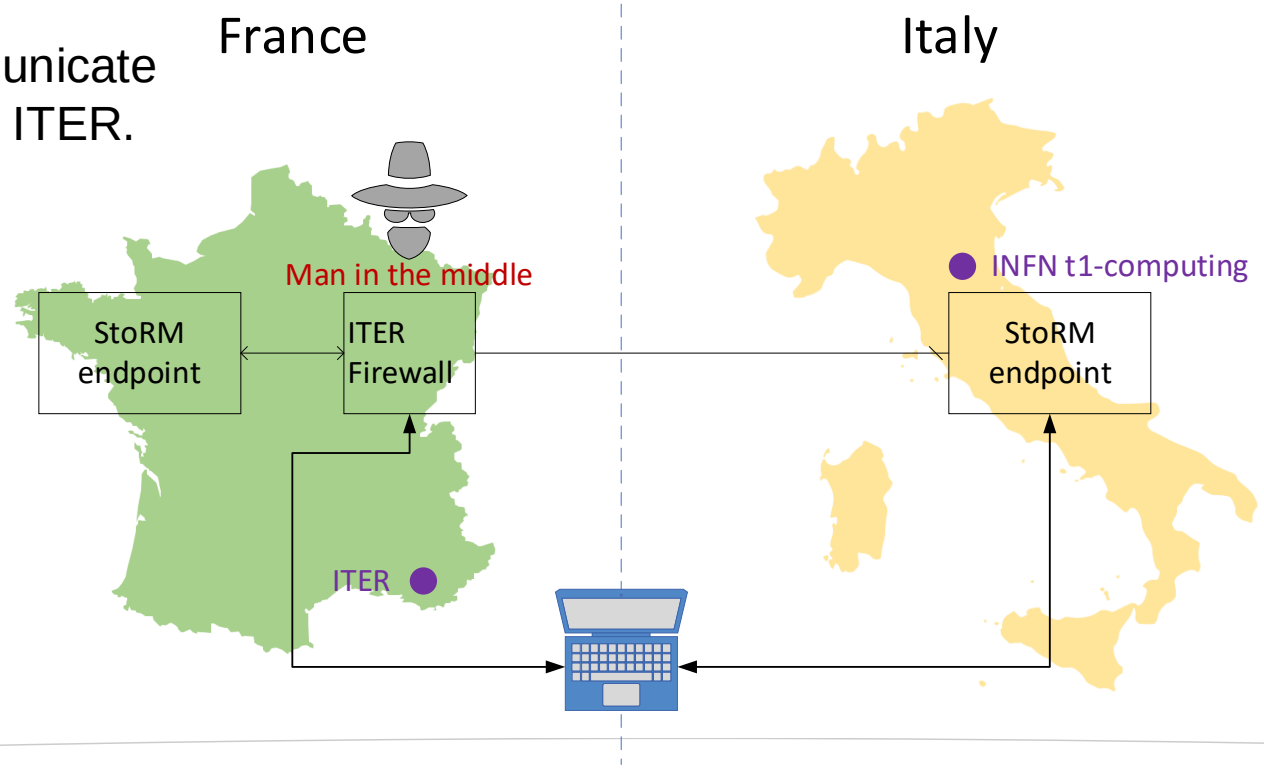
```
curl -X MKCOL http://4504uc-srv-0001:8085/local-sa/test-no-auth
```

Example for read content:

```
curl -I http://4504uc-srv-0001:8085/local-sa/test-no-auth
```

Summary. Discovered problems

1. Authentication problem exists, for tests with INFM instance we probably will use INFM token provider, bat we will need to think about ITER one for that kind of services.
2. From infrastructure perspective, to make client and server installation we need to add several RPM packages to our repositories.
3. Network setup required, because we cannot communicate between StoRM instances inside ITER and outside ITER.
4. Not up to date. (java 11, level CentOS7)
5. not RH8, not in perspective RH9

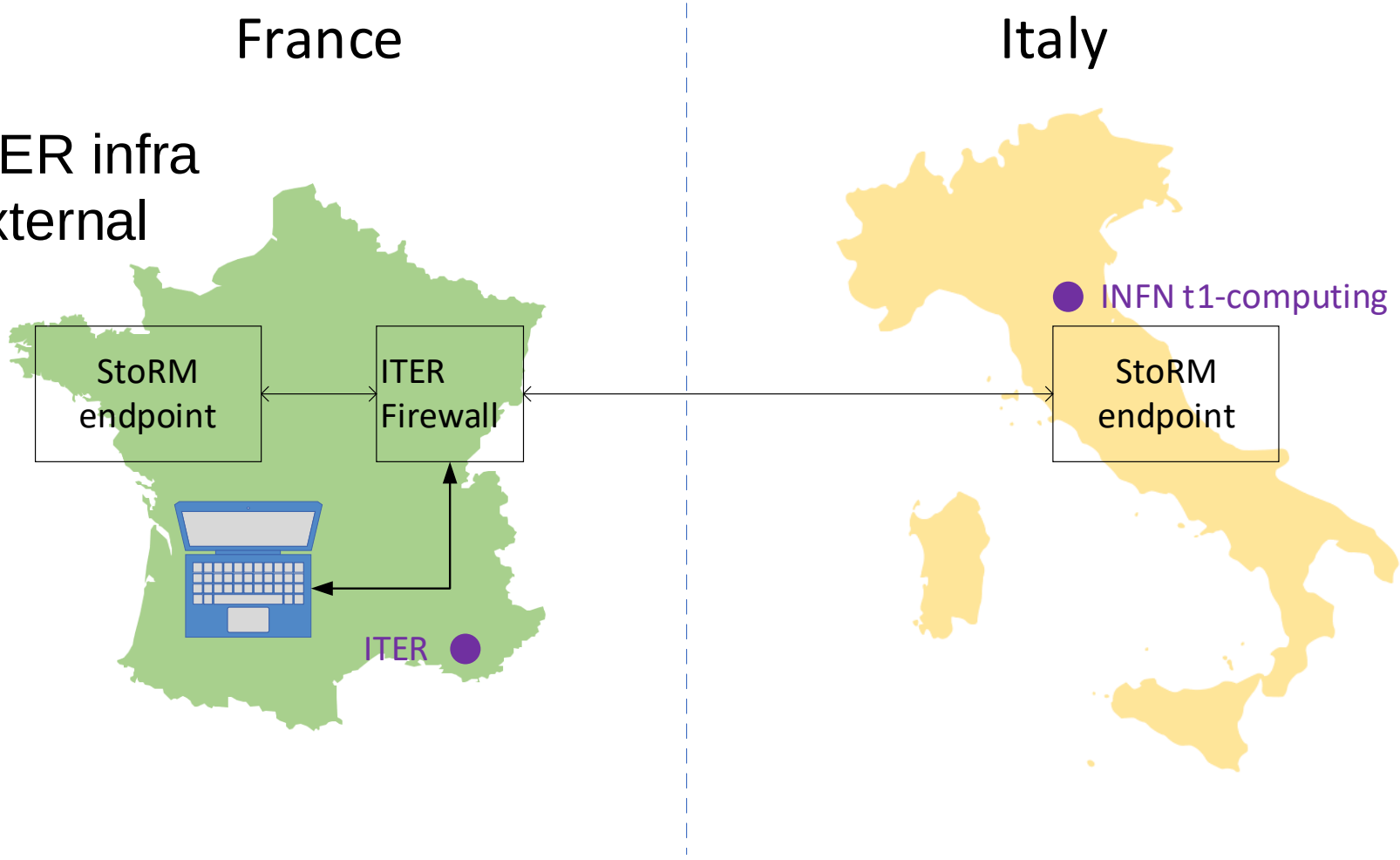


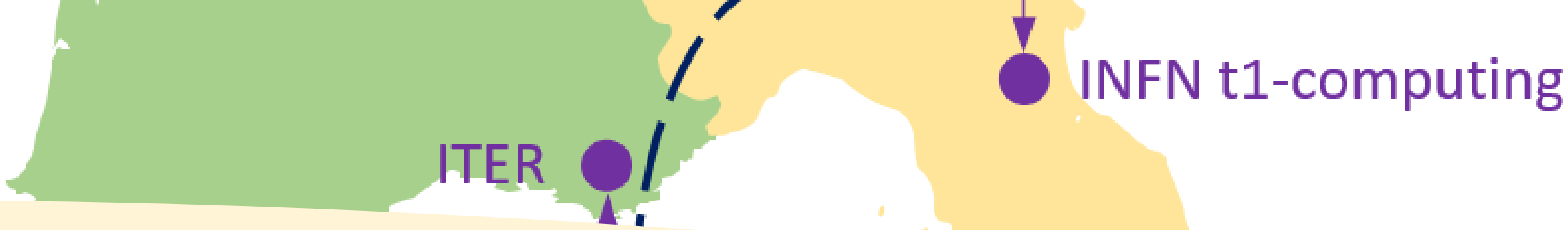
Summary. Main key points

We have:
Server instance in ITER infra
Client instance for external

We do not have:
Any **token provider**

What we want?





Thank you!

StoRM ITER TEST

ITER-INFM meeting

Lobes Leonid,
23.07.2024

iter
china eu india japan korea russia usa