Deploying federated services in eduroam with Moonshot

Grupos de trabajo de RedIRIS 2014, Madrid

Alejandro Pérez, Rafael Marín, Gabriel López

Departamento de Ingeniería de la Información y las Comunicaciones
University of Murcia

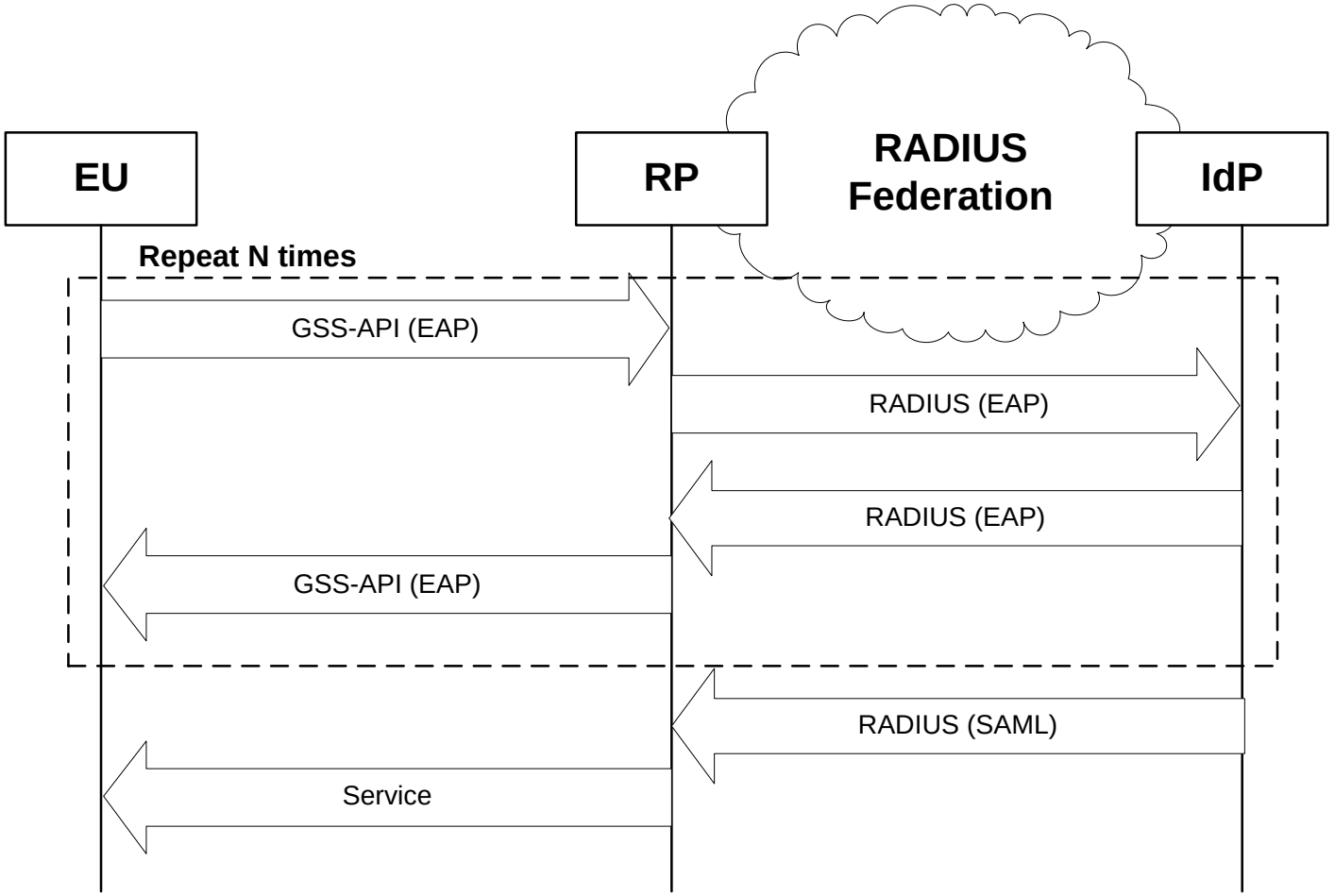
Motivation

- Identity federations
  - Trust relationships to identify end users
  - Usability and lower deployment costs
- Drawbacks
  - Defined for specific kinds of services
  - Use of different technologies
    - Access to the network service (e.g. eduroam) → RADIUS, Diameter...
    - Web applications → SAML, OpenID, OAuth…
  - Some services do not provide support for federation
    - Email, remote file access, remote terminal access…

What's Moonshot?

- Moonshot
  - Development of a technology to bring the identity federation concept to any kind of service (e.g. cloud, ftp, http, ssh…)
- Key components:
  - EU→ Wants to access a service
  - RP → Provides the service
  - IdP → Authenticate the end user and provides authorization information to the RP
- Key technologies:
  - GSS-API → Access control to the service (between EU and RP)
  - RADIUS → Federation (between RP and IdP)
  - SAML → Authorization (between RP and IdP)
  - EAP → User authentication (between EU and IdP)

What's Moonshot?



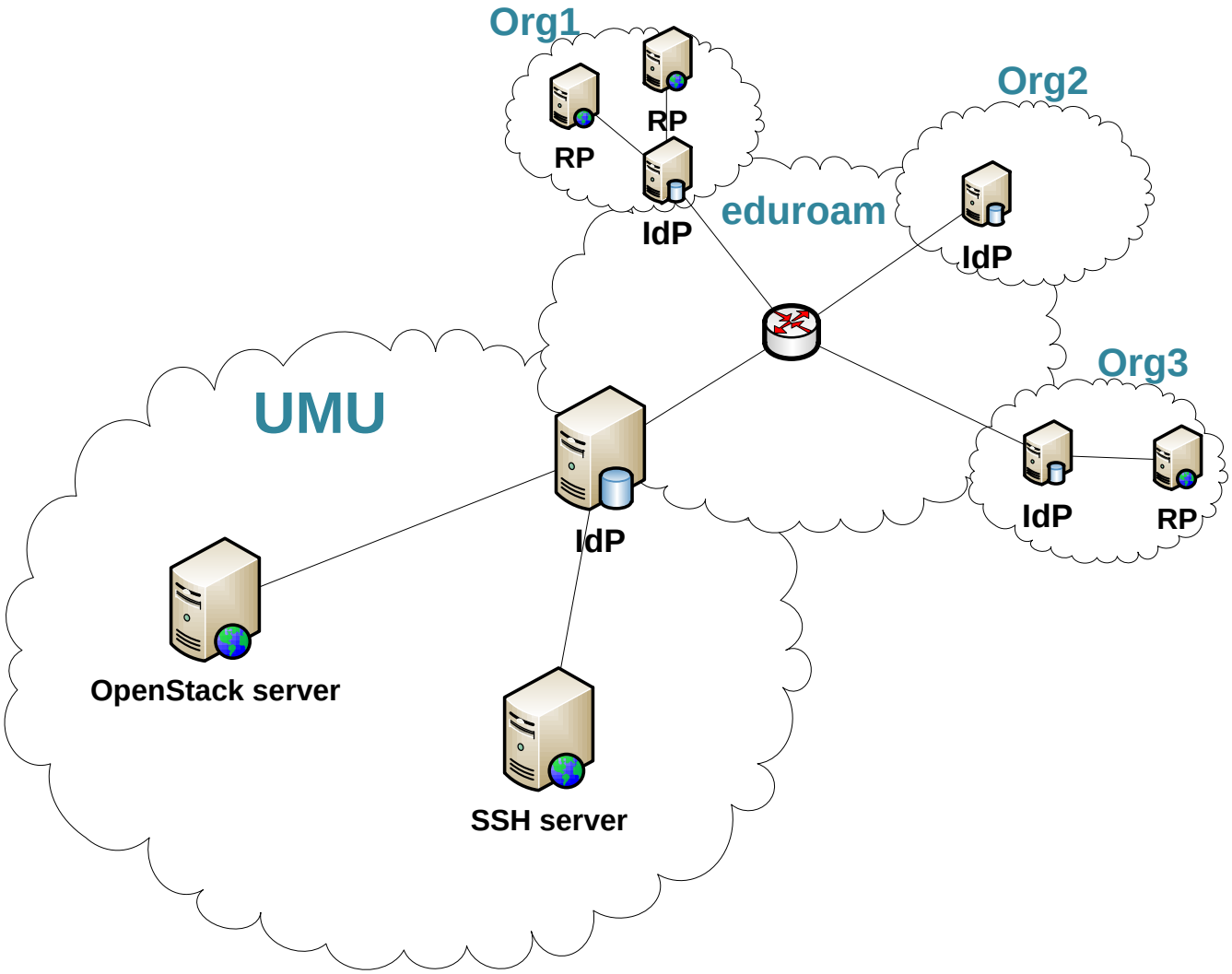
What's Moonshot?

- Partly performed within GN3 project
  - Participated by RedIRIS and UMU
- Being standardized within the IETF (ABFAB WG)
- Completely implemented, documented, and maintaned by the Moonshot community
  - https://community.ja.net/groups/moonshot

Deploying Moonshot

- The RADIUS infrastructure of eduroam is an ideal candidate to deploy Moonshot
  - Trust relationships are already established
  - A great number of interconnected organizations
- We'll see how to deploy the different components of Moonshot using this infrastructure
- Two practical examples, deployed at UMU:
  - SSH server allowing the access to the *federated* account to any member of the eduroam community **(GN3Plus)**
  - OpenStack server allowing the access to the *swifttenanttest1* tenant only to UMU's members, and the access to the *swifttenanttest2* tenant to any member of the eduroam community **(CLASSe)**

Deploying Moonshot



Deploying Moonshot - IdP

- Any current RADIUS server from the eduroam network can act as a Moonshot IdP…
  - But they will not send the SAML assertion
- To configure a new IdP:
  1. Install FreeRADIUS and connect it to the eduroam's infrastructure
  2. Create the required user accounts
  3. Configure FreeRADIUS to generate a SAML assertion:
     - Static → Fixed assertion template, filled with FreeRADIUS variables
     - Dynamic → Assertion generated with OpenSAML, filled with values obtained from different data bases (in development)

Examples #1 and #2: IdP

- Configure a new RADIUS server
  - UM's subdomain
  - moonshot.um.es
- Create a testing account
  - test@moonshot.um.es
- Configure the SAML assertion template
  - post-auth section of sites-enabled/default file

```
update reply {
 SAML-AAA-Assertion = "<saml:Assertion xmlns:saml='urn:oasis:names:tc:……."
 SAML-AAA-Assertion += "<saml:Conditions NotOnOrAfter='2015-03-19T08:30:00Z'/>"
 SAML-AAA-Assertion += "<saml:Issuer>moonshot.inf.um.es</saml:Issuer>"
 …….
```

Examples #1 and #2: IdP

```
<saml:Assertion xmlns:saml='urn:oasis:names:tc:SAML:2.0:assertion‘ ...>
    <saml:Conditions NotOnOrAfter='2015-03-19T08:30:00Z'/>
    <saml:Issuer>moonshot.um.es</saml:Issuer>
    <saml:Subject>
        <saml:NameID Format='urn:oasis:names:tc:SAML:2.0:nameid-format:transient'>
            %{%{reply:User-Name}:-%{request:User-Name}}
        </saml:NameID>
    </saml:Subject>
    <saml:AttributeStatement>
        <saml:Attribute Name='studentcard‘ ...>
            <saml:AttributeValue>Student</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name='affiliation‘ ...>
            <saml:AttributeValue>umu</saml:AttributeValue>
        </saml:Attribute>
    </saml:AttributeStatement>
</saml:Assertion>
```

Example:
test@moonshot.um.es

Deploying Moonshot - RP

- Any application supporting the GSS-API should work with Moonshot
  - Although some of them are badly programmed and require small adjustments (e.g. OpenSSH)
- It will be needed to:
  1. Install Moonshot's code in the RP
  2. Configure a RADIUS proxy connected to the eduroam's infrastructure
  3. Configure attribute mapping (authorization)
     - Convert RADIUS and/or SAML attributes into the application's specific attributes

Example #1: SSH server

- Configure the machine:
  - moonshot-ssh.inf.um.es
- Install Moonshot
- Install OpenSSH server patched for Moonshot
  - Available from the Moonshot repositories
- Configure the RADIUS proxy
  - moonshot.um.es
- Configure attribute mapping
  - If TRUE →
    - OpenSSH.local_login_user := federated
  - Does not require SAML assertion
  - This authorizes any user to access to the account federated@moonshot-ssh.inf.um.es

Example #2: OpenStack server

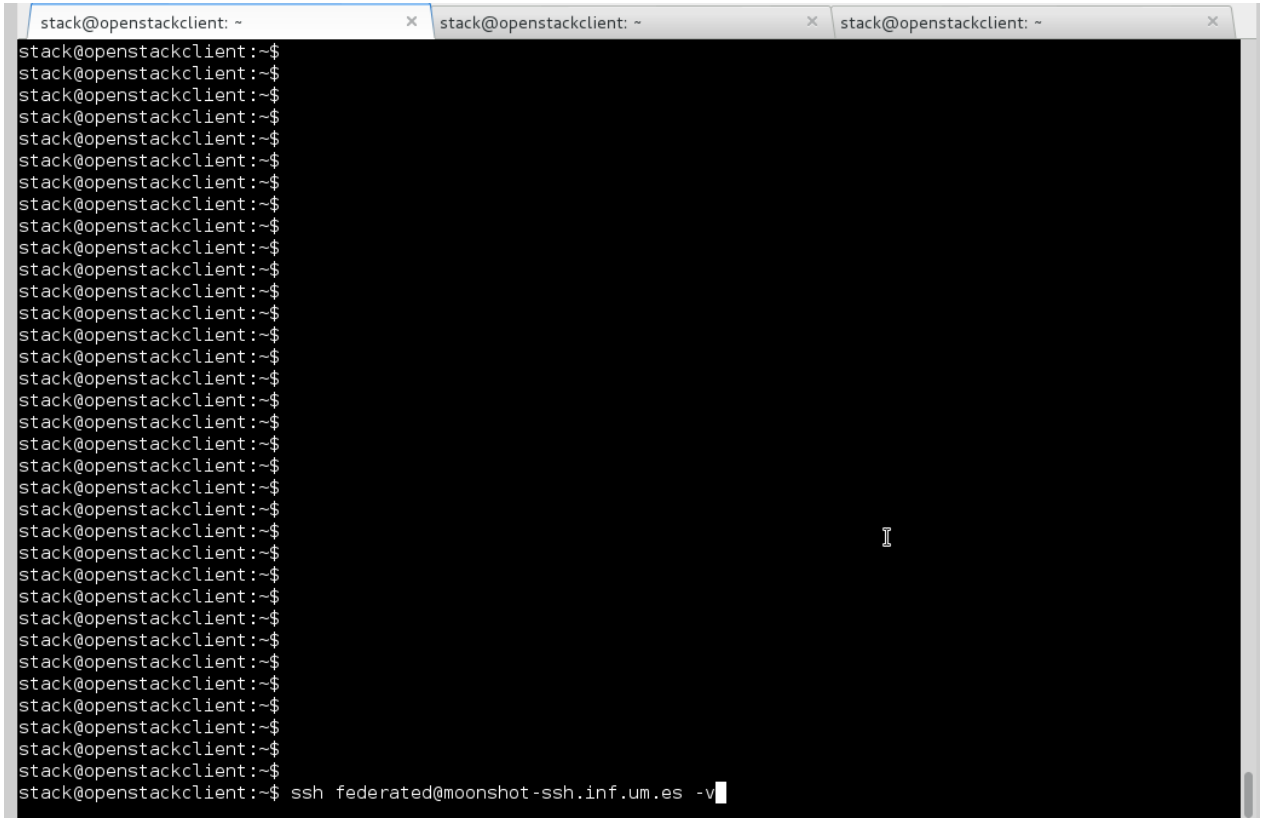
- Configure the machine
  - classe1.qalab.geant.net
- Install Moonshot
- Install OpenStack server with support for GSS-API
  - https://github.com/kwss/keystone
- Configure the RADIUS proxy
  - moonshot.um.es
- Configure attribute mapping
  - If *SAML.affiliation* == umu →
    - OpenStack.tenant := swifttenanttest1
  - Else →
    - OpenStack.tenant := swifttenanttest2

Deploying Moonshot - EU

- Any application supporting GSS-API should work with Moonshot
- It will be needed to:
  1. Install Moonshot code
  2. Try to access the service
  3. Introduce or select the desired identity from the selector

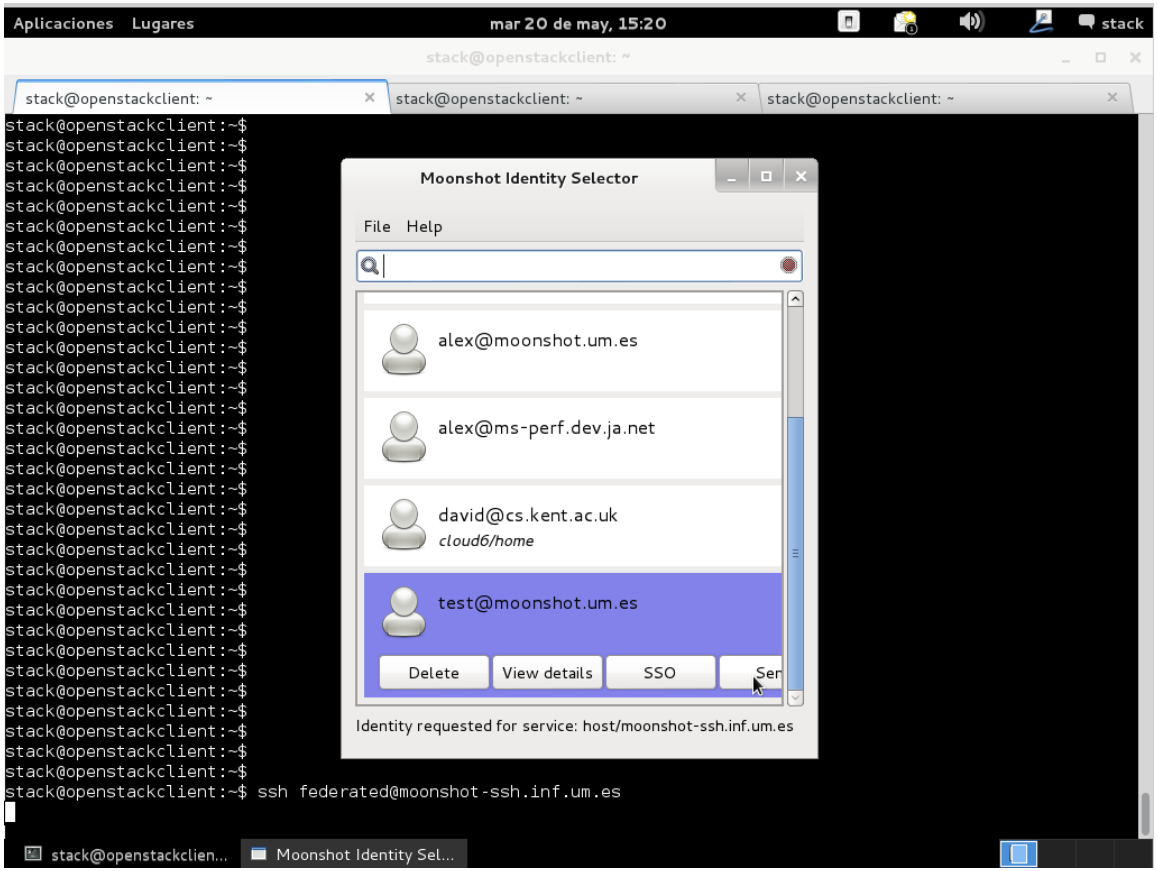
Example #1: SSH client

1. Install Moonshot
2. Access to the service
   - ssh federated@moonshot-ssh.inf.um.es



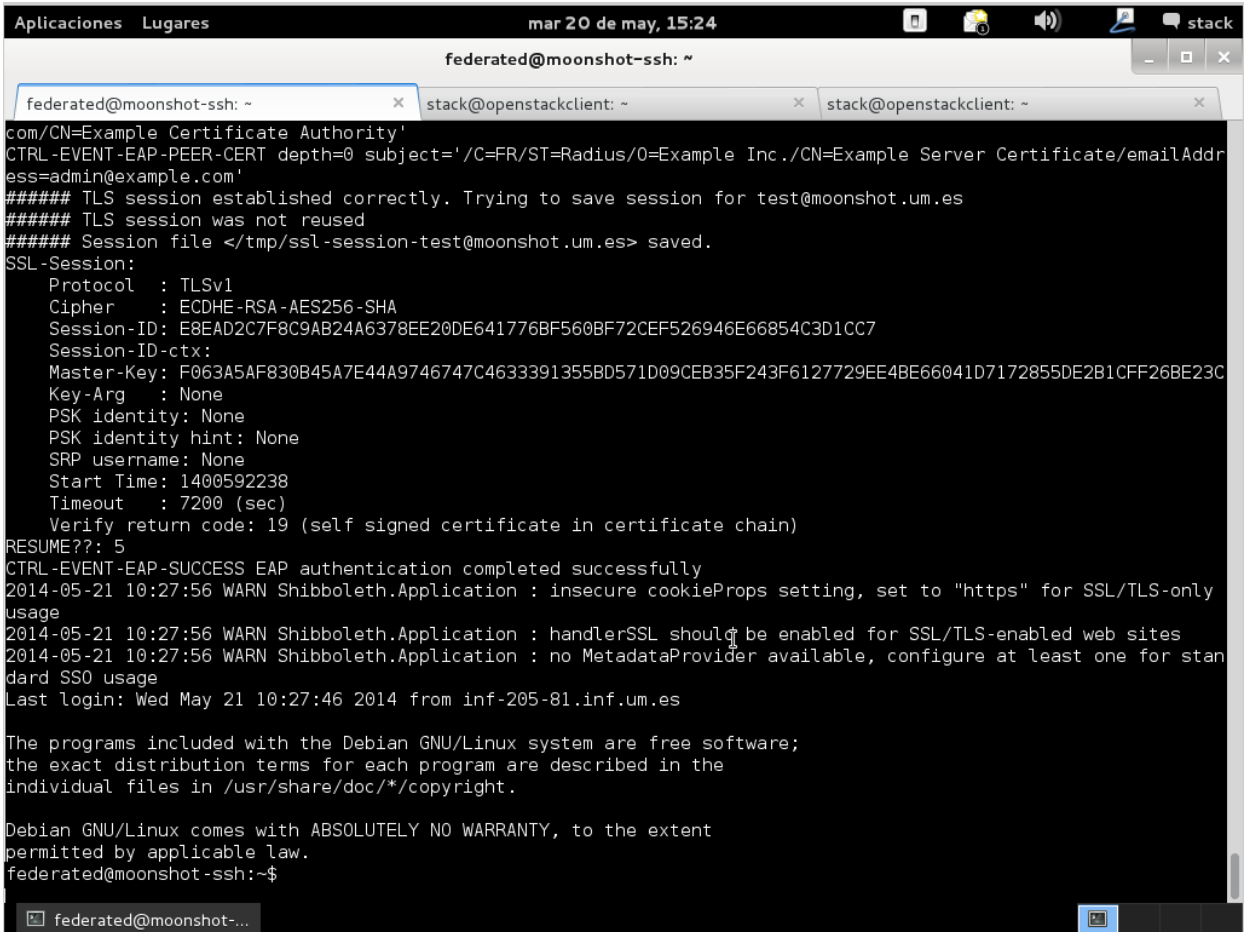
Example #1: SSH client

3. Select the identity
   - test@moonshot.um.es
   - Or any other identity valid within eduroam



Example #1: SSH client

4. Access to the requested service

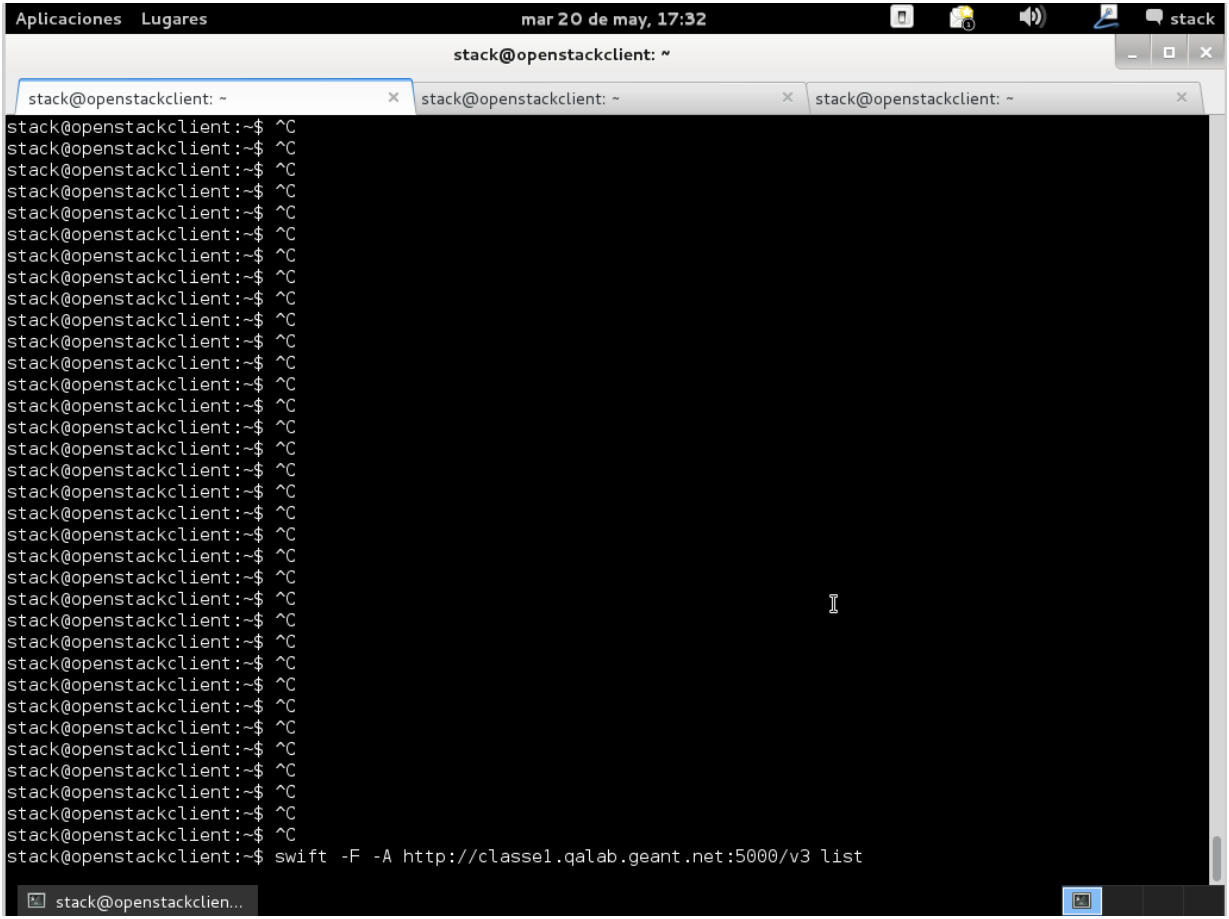


Example #2: OpenStack client

1. Install Moonshot
2. Install the OpenStack client with support for the GSS-API
   - http://sec.cs.kent.ac.uk/demos/keystone.html

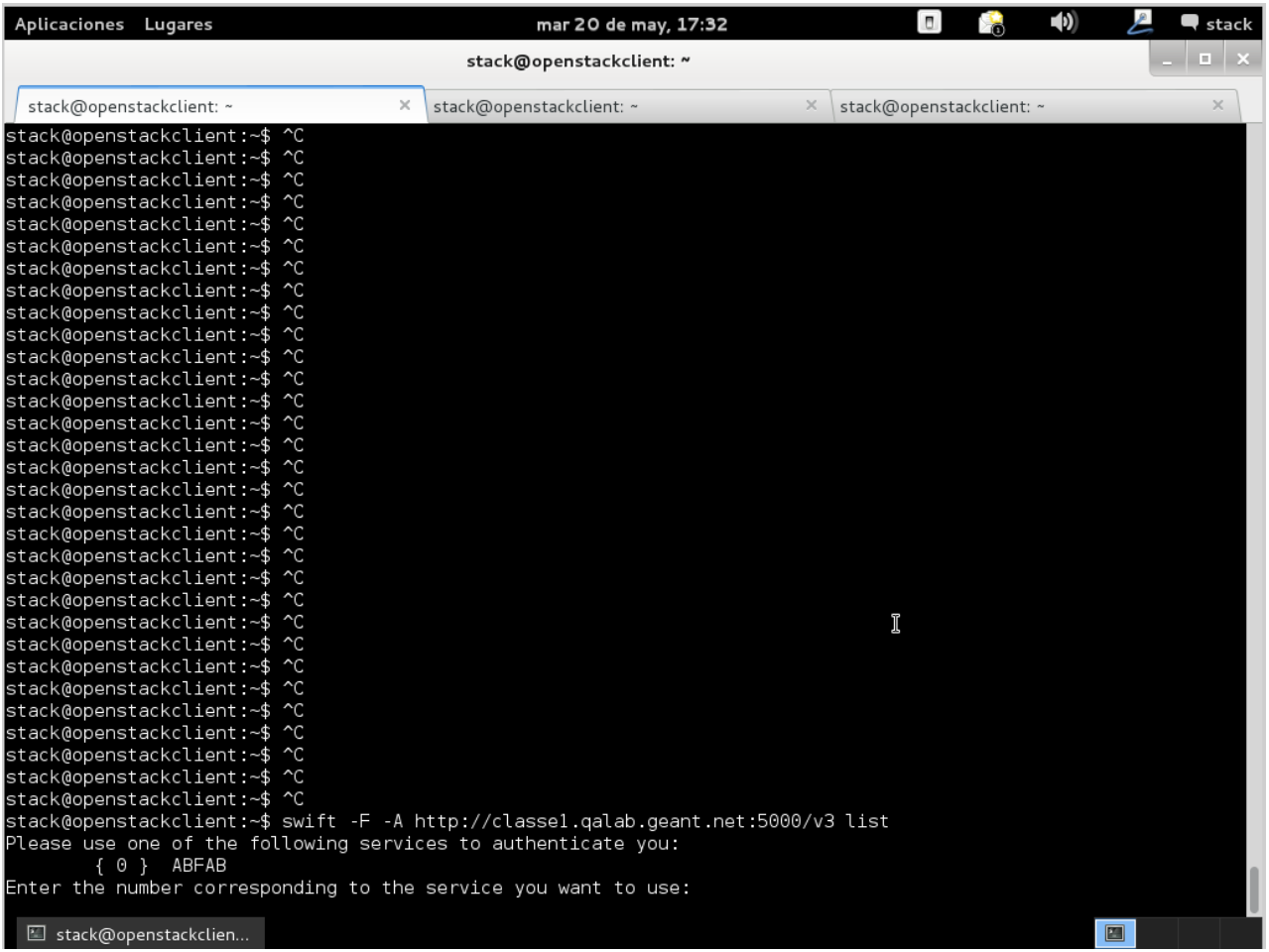
Example #2: OpenStack client

3. Access to the service
   - swift -F -A http://classe1.qalab.geant.net:5000/v3 list



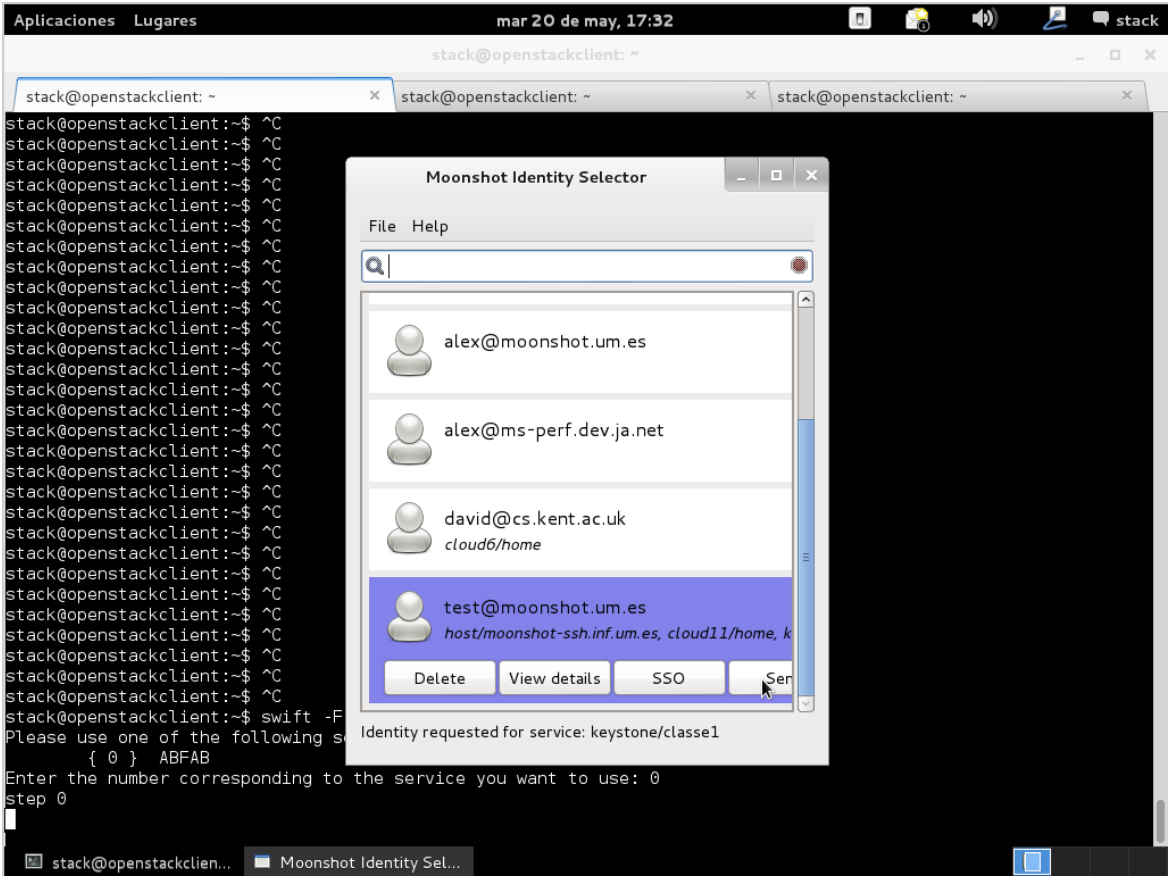
Example #2: OpenStack client

4. Select Moonshot-based authentication



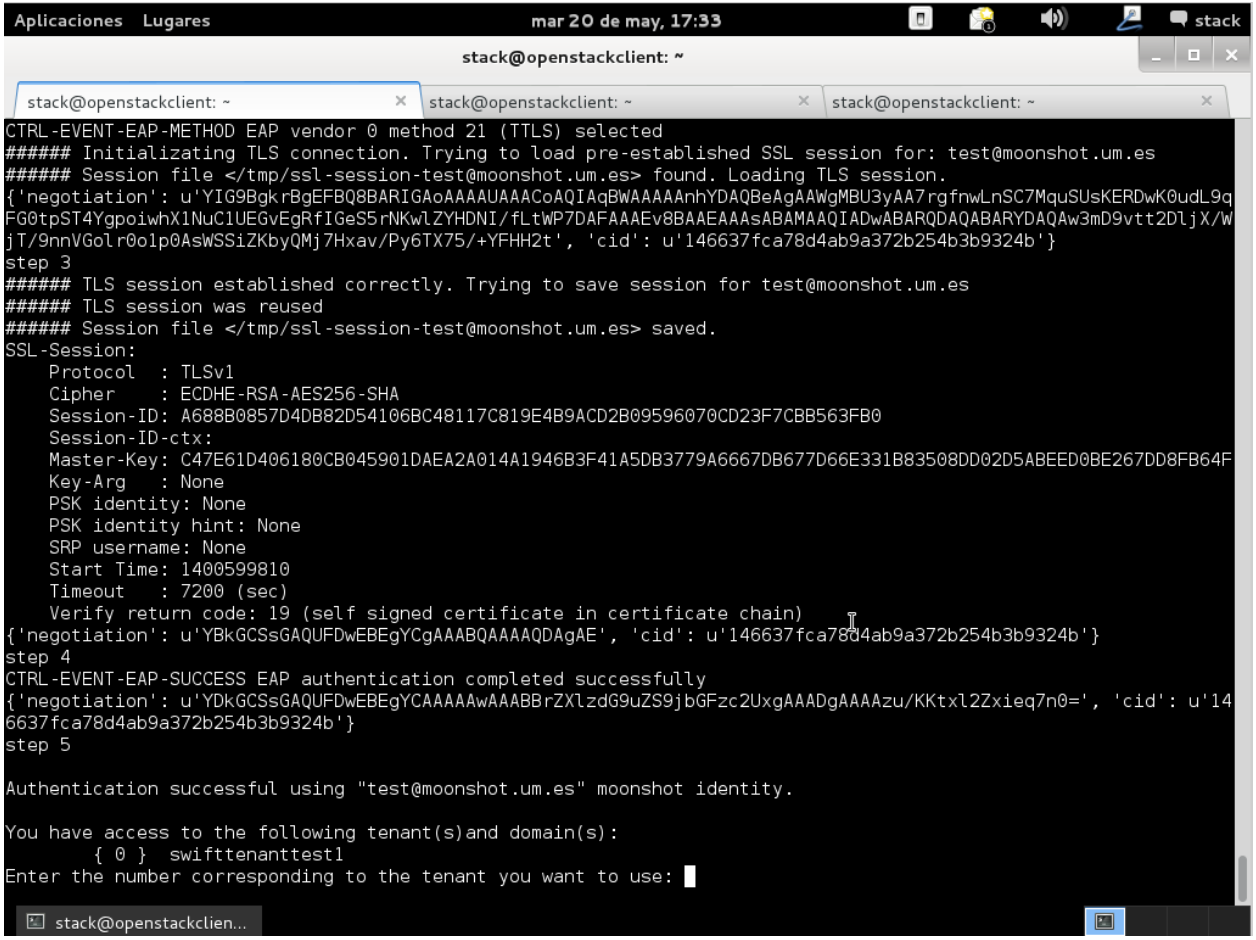
Example #2: OpenStack client

5. Select the desired identity
   - test@moonshot.um.es
   - Or any other identity valid within eduroam



Ejemplo 2: Cliente OpenStack

6. Get access to the *tenant*



Thank you for your attention

Any further question?