Desplegando servicios federados en eduroam con Moonshot

Grupos de trabajo de RedIRIS 2014, Madrid

Alejandro Pérez, Rafael Marín, Gabriel López

Departamento de Ingeniería de la Información y las Comunicaciones
Universidad de Murcia

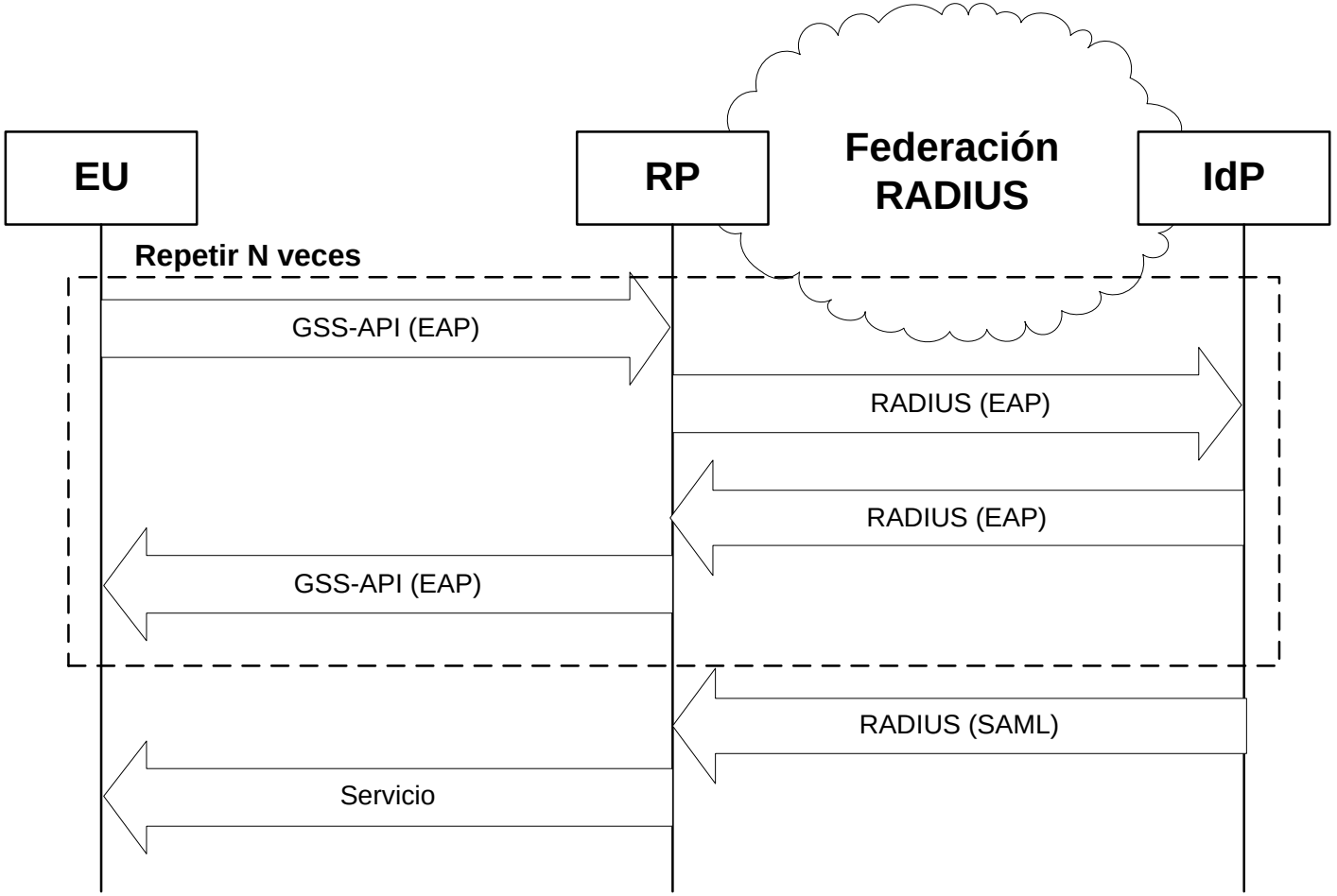
Motivación

- Federaciones de identidad
  - Relaciones de confianza para identificar usuarios
  - Usabilidad y menor coste de despliegue
- Inconvenientes
  - Definidas para tipos de servicio específicos
  - Uso de tecnologías diferentes
    - Acceso a la red (p.ej. eduroam) → RADIUS, Diameter...
    - Servicios web → SAML, OpenID, OAuth…
  - Algunos servicios no disponen de soluciones de federación
    - Correo electrónico, acceso remoto a ficheros, acceso a terminal remoto…

¿Qué es Moonshot?

- Moonshot
  - Desarrollo de una tecnología para llevar el concepto de identidad federada a cualquier tipo de servicio (cloud, ftp, http, ssh…)
- Elementos clave:
  - EU→ Quiere acceder a un servicio
  - RP → Proporciona el servicio
  - IdP → Autentica al usuario y proporciona información de autorización al RP
- Tecnologías clave:
  - GSS-API → Control de acceso a servicios (entre EU y RP)
  - RADIUS → Federación (entre RP e IdP)
  - SAML → Autorización (entre RP e IdP)
  - EAP → Autenticación de usuario (entre EU e IdP)

¿Qué es Moonshot?



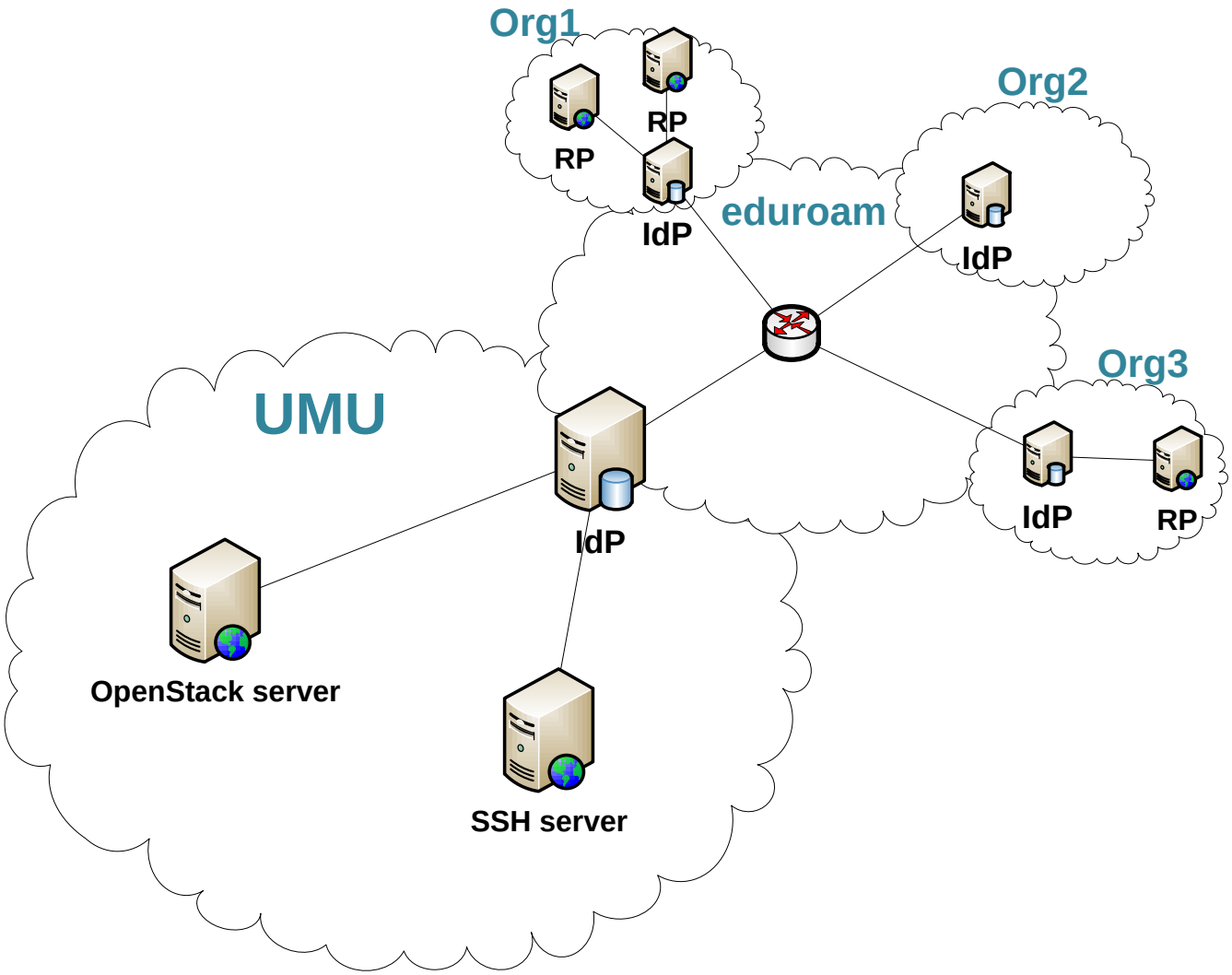
¿Qué es Moonshot?

- Realizado en parte dentro del proyecto GN3
  - Participado por RedIRIS y la UMU
- En proceso de estandarización dentro del IETF (ABFAB WG)
- Completamente implementado, documentado y mantenido por la comunidad Moonshot
  - https://community.ja.net/groups/moonshot

Desplegando Moonshot

- La infraestructura RADIUS de eduroam es una candidata ideal para el despliegue de Moonshot
  - Las relaciones de confianza ya están establecidas
  - Multitud de organizaciones interconectadas
- Veremos cómo desplegar los diferentes componentes de Moonshot usando esta infraestructura
- Dos ejemplos prácticos, desplegados en UMU:
  - Servidor SSH que permite el acceso a la cuenta *federated* a cualquier miembro de la comunidad eduroam **(GN3Plus)**
  - Servidor OpenStack que permite el acceso al tenant *swifttenanttest1* sólo a los miembros de UMU, y el acceso a *swifttenanttest2* a cualquier miembro de la comunidad *eduroam* **(CLASSe)**

Desplegando Moonshot



Desplegando Moonshot - IdP

- Cualquier servidor RADIUS actual de eduroam pueden actuar como IdPs Moonshot…
  - Pero no envían la sentencia SAML
- Para configurar un IdP nuevo:
  1. Instalar FreeRADIUS y conectarlo a la infraestructura eduroam
  2. Crear las cuentas de usuario deseadas
  3. Configurar FreeRADIUS para que genere una sentencia SAML
     - Estática → Plantilla de sentencia fija, rellena con variables FreeRADIUS
     - Dinámica → Sentencia generada con OpenSAML, rellena con valores obtenidos de diferentes bases de datos (en desarrollo)

Ejemplo 1 y 2: IdP

- Configuramos un nuevo servidor RADIUS
  - Subdominio de la UM
  - moonshot.um.es
- Creamos una cuenta de pruebas
  - test@moonshot.um.es
- Configuramos la plantilla para la sentencia SAML de forma estática
  - Sección post-auth del fichero sites-enabled/default

```
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>"
 …….
```

Ejemplo 1 y 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>
```

Ejemplo:
test@moonshot.um.es

Desplegando Moonshot - RP

- Cualquier aplicación que soporte GSS-API debe funcionar con Moonshot
  - Aunque algunas están mal programadas y requieren pequeños ajustes (ej. OpenSSH)
- Será necesario:
  1. Instalar código de Moonshot en el RP
  2. Configurar un proxy RADIUS conectado a la infraestructura eduroam
  3. Configurar mapeo de atributos (autorización)
     - Convertir atributos RADIUS y/o SAML en atributos específicos de la aplicación

Ejemplo 1: Servidor SSH

- Configuramos la máquina
  - moonshot-ssh.inf.um.es
- Instalamos Moonshot
- Instalamos servidor OpenSSH parcheado para Moonshot
  - Disponible con el propio código de Moonshot
- Configuramos el proxy RADIUS
  - moonshot.um.es
- Configuramos el mapeo de atributos
  - Si TRUE →
    - OpenSSH.local_login_user := federated
  - No requiere sentencia SAML
  - Esto autoriza a cualquier usuario a acceder a la cuenta federated@moonshot-ssh.inf.um.es

Ejemplo 2: Servidor OpenStack

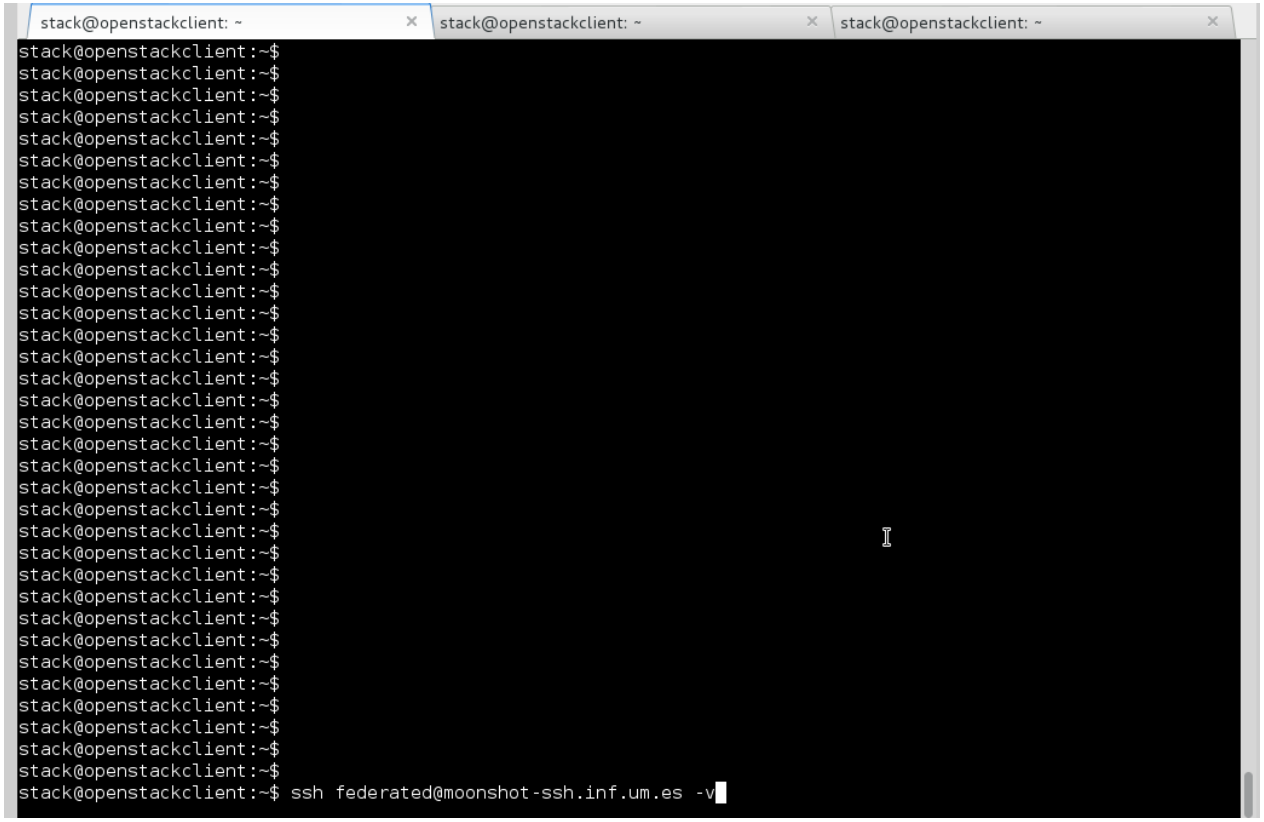
- Configuramos la máquina
  - classe1.qalab.geant.net
- Instalamos Moonshot
- Instalamos servidor OpenStack con soporte para GSS-API
  - https://github.com/kwss/keystone
- Configuramos el proxy RADIUS
  - moonshot.um.es
- Configurar mapeo de atributos
  - Si *SAML.affiliation* == umu →
    - OpenStack.tenant := swifttenanttest1
  - Si no →
    - OpenStack.tenant := swifttenanttest2

Desplegando Moonshot - EU

- Cualquier aplicación que soporte GSS-API debe funcionar con Moonshot
- Será necesario:
  1. Instalar código de Moonshot
  2. Intentar acceder al servicio
  3. Introducir o seleccionar la identidad a usar

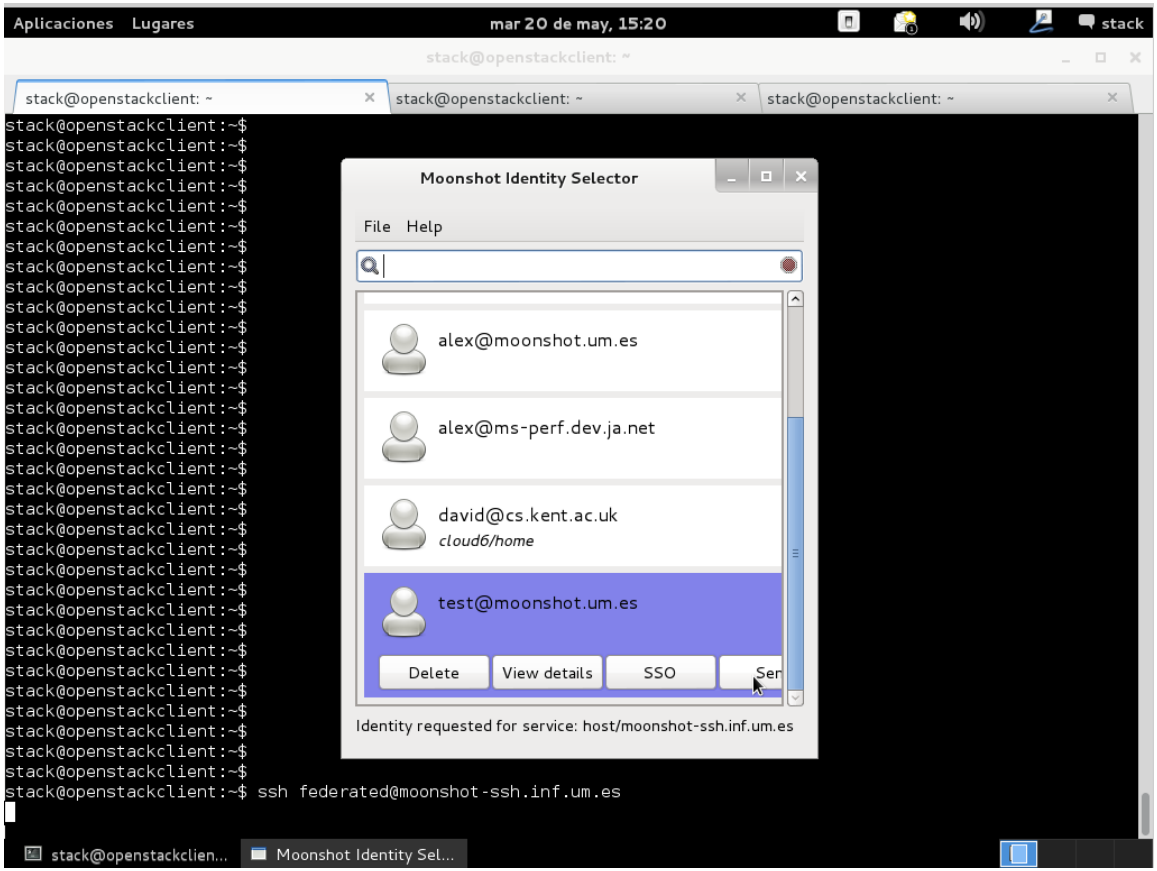
Ejemplo 1: Cliente SSH

1. Instalamos Moonshot
2. Accedemos al servicio
   - ssh federated@moonshot-ssh.inf.um.es



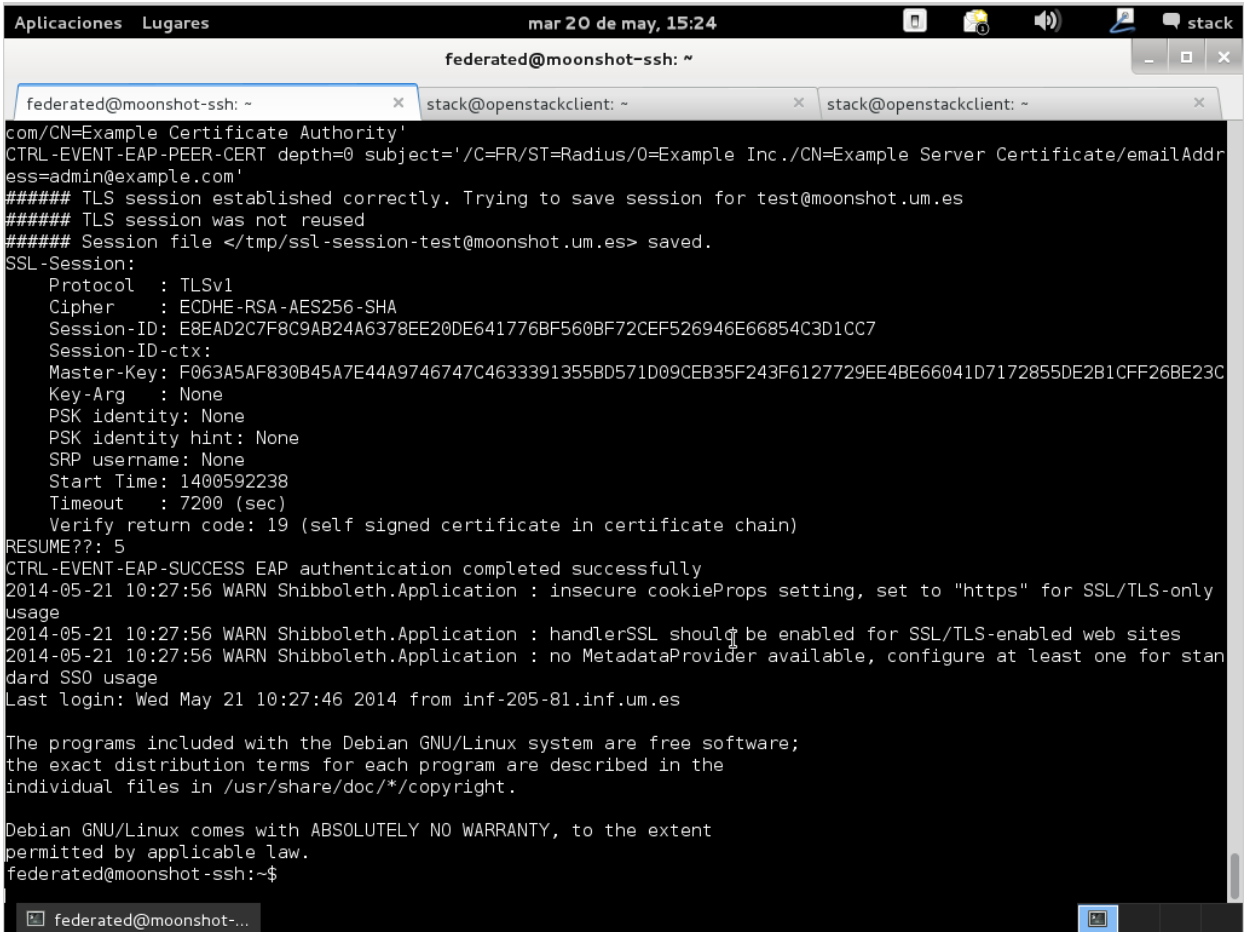
Ejemplo 1: Cliente SSH

3. Seleccionamos la identidad a utilizar
   - test@moonshot.um.es
   - O cualquier otra identidad válida en eduroam



Ejemplo 1: Cliente SSH

4. Accedemos al servicio solicitado

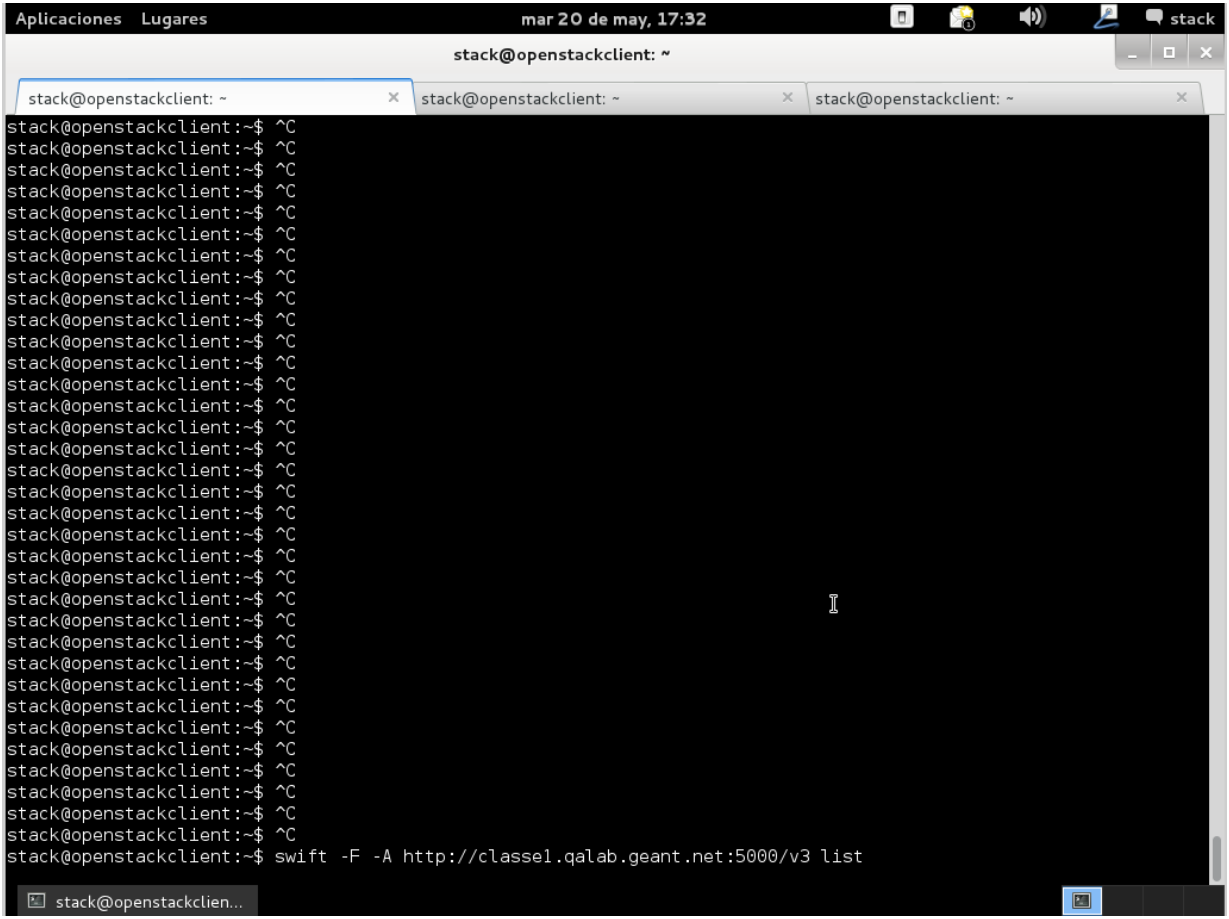


Ejemplo 2: Cliente OpenStack

1. Instalamos Moonshot
2. Instalamos el cliente OpenStack con soporte para GSS-API
   - http://sec.cs.kent.ac.uk/demos/keystone.html

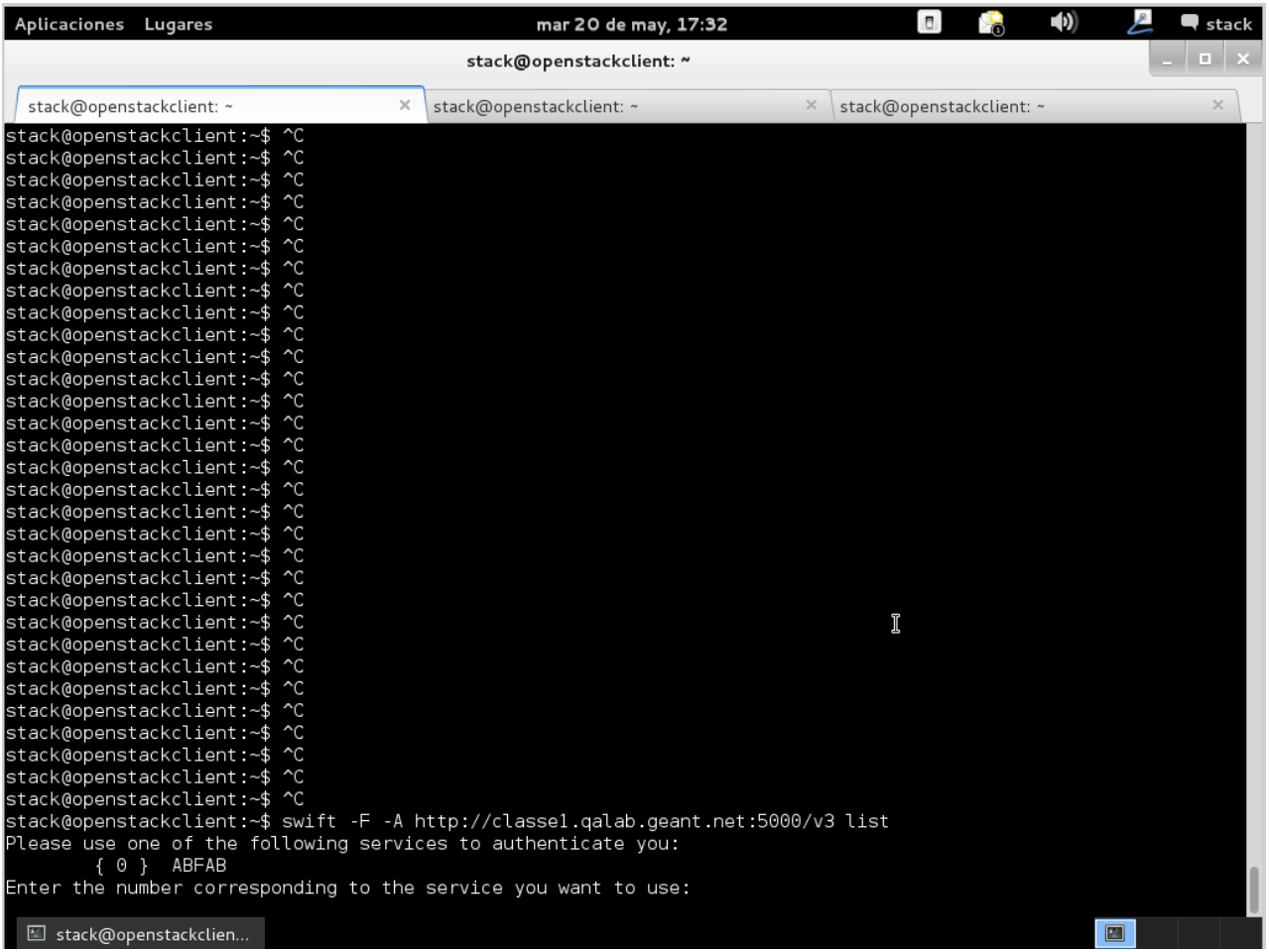
Ejemplo 2: Cliente OpenStack

3. Accedemos al servicio
   - swift -F -A http://classe1.qalab.geant.net:5000/v3 list



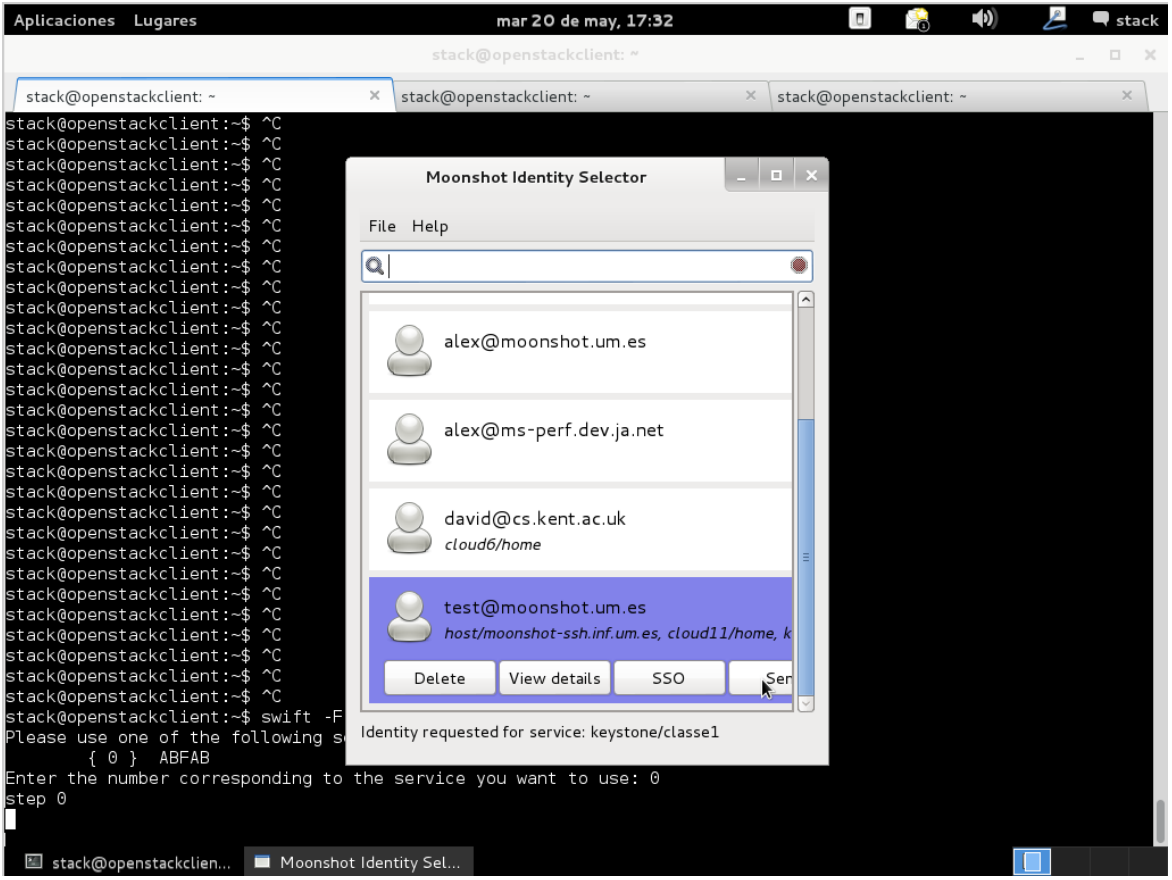
Ejemplo 2: Cliente OpenStack

4. Seleccionamos autenticación Moonshot



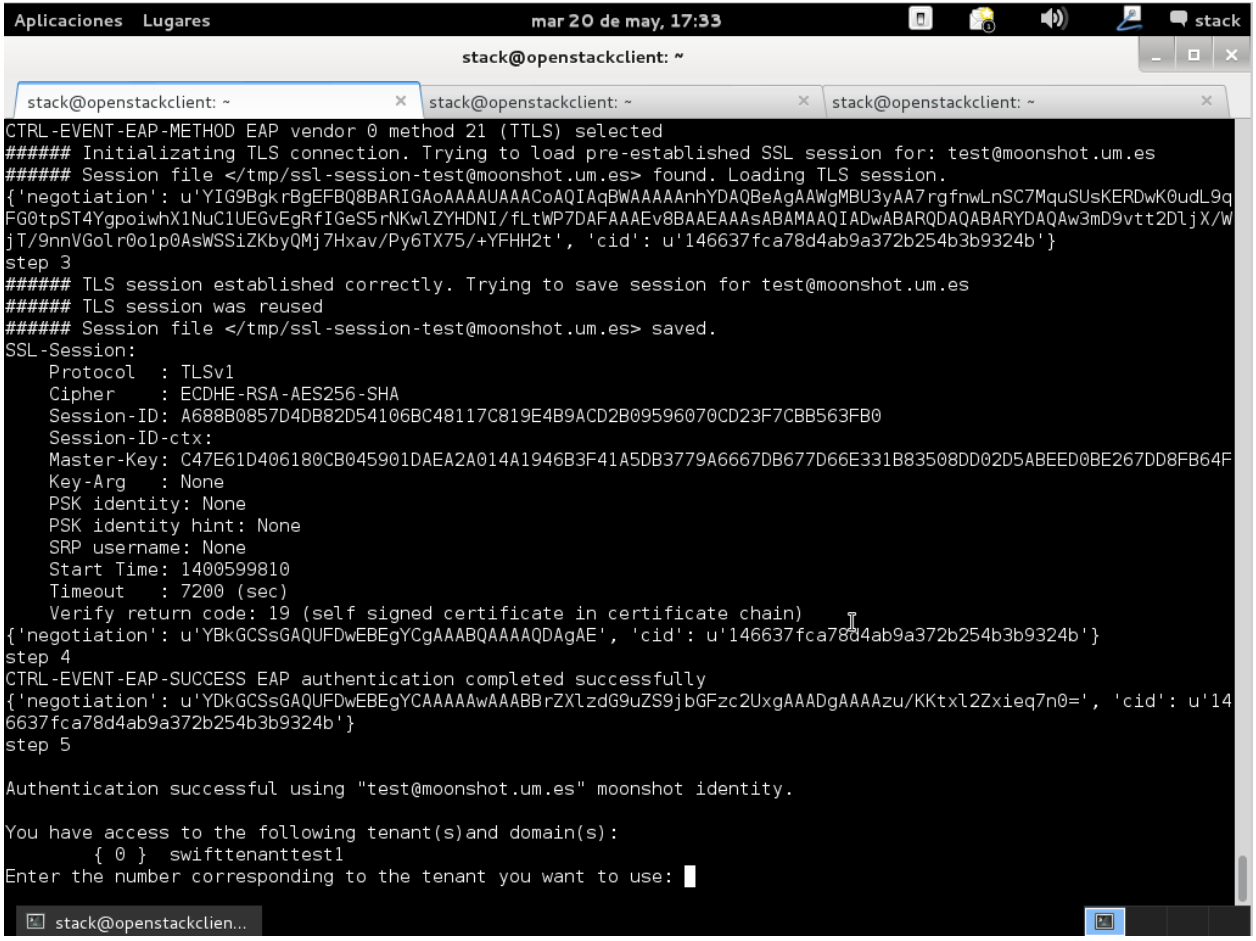
Ejemplo 2: Cliente OpenStack

5. Seleccionamos la identidad a utilizar
   - test@moonshot.um.es
   - O cualquier otra identidad válida en eduroam



Ejemplo 2: Cliente OpenStack

6. Obtenemos acceso al *tenant* correspondiente



Muchas gracias por su atención

¿Alguna pregunta?