Jisc

Moonshot

Workshop on Federated Identity and (OpenStack) Cloud Services - SWITCH

ABFAB - Federated access beyond web

Why?

- You've heard of eduroam
  - Federated network access
- You've heard of Shibboleth, eduGAIN
  - Federated web access
- Now we have Moonshot
  - Bridges gap between network + web
- It is finally here!
  - After 5 years of work, Jisc Assent launched 25/03/15

Federated access beyond the web

The scenario

- User Paul Jones, biologist, Oxford University
  - Collaborates with research centres in Harwell, Cambridge, Berlin, Boston
- Has to remember ≥5 sets of usernames + passwords
  - Various requirements (length, complexity)
  - Easiest to remember: Writes them down
- Wouldn't it be nice if there was only **one** set?
- With Assent and Moonshot, that's possible!

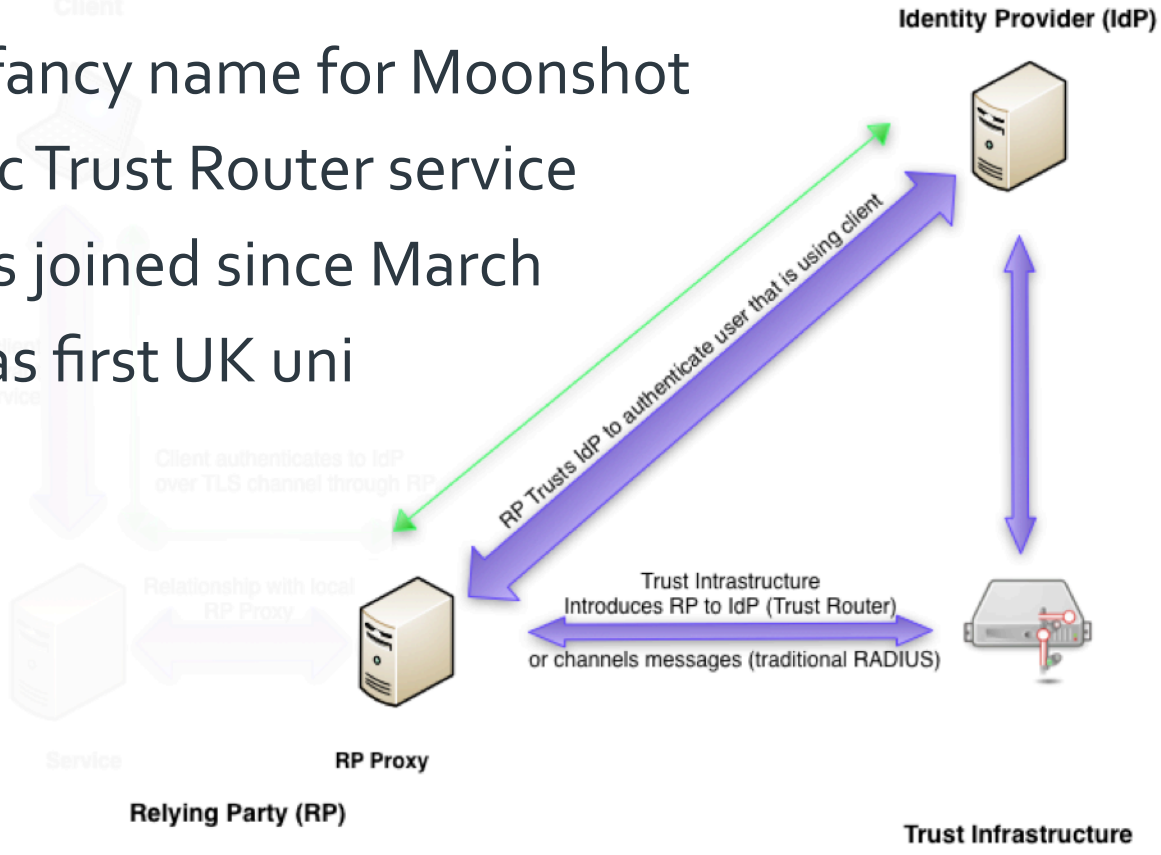
Moonshot
Huh? What's that?

- Moonshot is a set of IETF standards
  - RFC7055, RFC7056, several drafts
  - Long term project for Jisc (5+ years)
- It uses proven technologies
  - RADIUS, SAML (OASIS/Shibboleth), GSSAPI (MIT)
- Technology underpins Jisc Assent service

Jisc Assent

What is Assent?

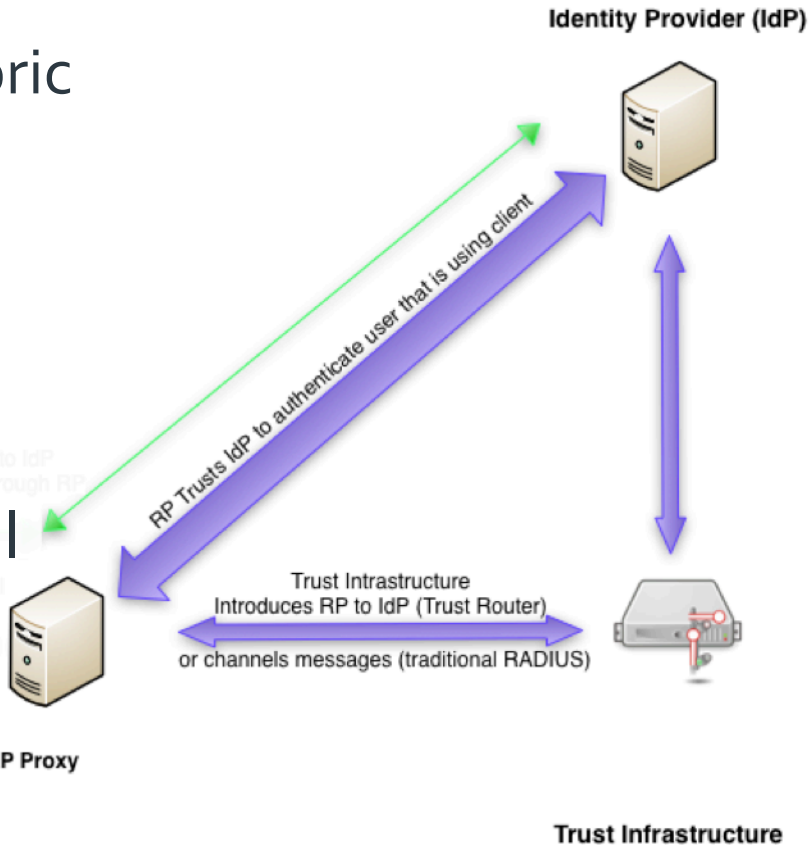
- Assent is **not** a fancy name for Moonshot
- Assent is the Jisc Trust Router service
- 10 organisations joined since March
  - Cambridge was first UK uni



Jisc Assent

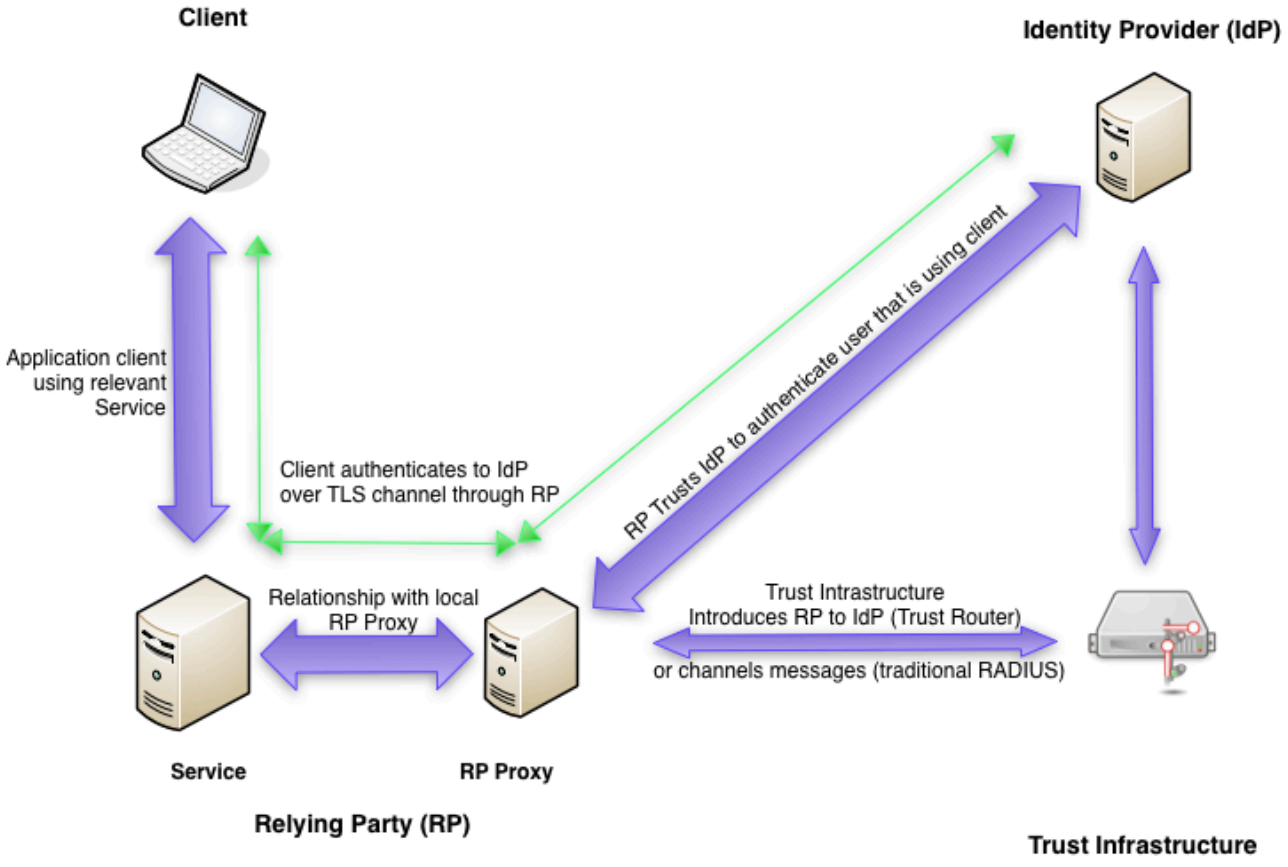
What does Assent do?

- Assent provides the trust fabric
  - You trust Assent
  - Someone else does too
  - Assent can introduce you two to each other
- Managed through web portal
- Federated, of course



Moonshot

How it works – The diagram



Moonshot
How it works (1/2)

- Client speaks to the Service over GSSAPI (EAP, encrypted)
- Service speaks to RP Proxy over TLS (RADIUS)
- RP Proxy contacts Trust Router to find IdP (TID protocol)
  - RP Proxy and IdP identify themselves to TR (Moonshot)
  - TR checks trust path if IdP + RP Proxy may talk
  - If yes, TR gives RP Proxy + IdP half a key (DH)
- RP Proxy contacts IdP over TLS (RADIUS)

Moonshot

How it works (2/2)

- RP Proxy passes EAP auth to IdP over TLS (RADIUS)
- IdP authenticates request, builds response
- IdP responds to RP Proxy over TLS (RADIUS)
- RP Proxy processes response
  - Does local authorization decisions
  - Does local account mapping
- RP Proxy responds to Service over TLS (RADIUS)
- Service logs Client in – User can now do stuff

Moonshot
Required components

- Moonshot client
  - Needed on client device, RP Proxy, IdP
  - Windows: Moonshot SSP and its successor
  - Linux: moonshot-gss-eap, moonshot-ui
- Moonshot TID service (trust_router)
  - Needed on RP Proxy, IdP
- FreeRADIUS v3.0.7 or higher (built with TID support)
  - Needed on RP Proxy, IdP

Moonshot
Supported platforms

- Linux
  - RedHat 6.x, CentOS 6.x (RHEL 7 in the works)
  - Debian 7, Ubuntu 12.x (Ubuntu 14 requires mixed repos)
- Windows
  - Windows 7, Windows 8, Windows 8.1, Windows 10
- Mac OS X is a high priority
  - In progress
- Mobile: Android pilot

Assent + Moonshot Progress

What's happened since going live?

- Development + bug fixing (business as usual)
- Software support
  - OpenSSH: Works, patches exist for v5 (PS), v6 (NIIF), v7 (NCSA)
    - Just need them in the upstream now
  - mod_auth_gssapi: Apache module works (v2.2 and v2.4)
  - gss_web: Browser plugin + Apache module done
  - myProxy: Jim Basney (NCSA) confirms it works
  - NFSv4: Daniel Kouřil (CESNET) made it work
  - putty 0.6x: Close to getting Moonshot support
  - Browsers natively support GSS-API, so all ok (except Safari)

Assent + Moonshot – Future

What do we still need?

- We identified credential delegation as being important
  - Priority for HPC + Grid
  - Better web access (GSSAPI over Javascript)
- More software support
- Do you have any use cases?
  - We want to know!

Ongoing European (GÉANT) Pilots
What's happening?

- Pilots and projects:
  - Universidad de Murcia (with University of Kent): OpenStack (Liberty)
  - UM: KDC Moonshot AuthN + ticket forwarding
  - CSC (Finland – iRODS + grid computing)
- Trust Router routing across NRENs
  - RÉNATER, REDIRIS et al.
- Building interest in other communities across Europe

Case studies
FARR Institute

- Medical research e-Infrastructure provider in the UK
- Safe Share project
- Pilots:
  - HPC – Universities of Leeds, Manchester, Sheffield
    - Accessing N8 cluster using home credentials
  - VDI – University of Swansea
    - OpenStack: In progress
  - eMedLab – Accessing datasets with home credentials
    - Sanger + Francis Crick, EMBL-EBI, UCL, KCL, Queen Mary
    - Leading to other pilots with Swansea (CLIMB) and Oxford
  - Oxford – University of Oxford's medical sciences
    - Using eMedLab to demo secure access to owners of live data set repos

Questions

What questions have you got for us?

- The Assent service
  - http://www.jisc.ac.uk/assent
- Moonshot (technology) wiki:
  - https://wiki.moonshot.ja.net
- Contacting me:
  - My email: stefan.paetow@jisc.ac.uk
  - Skype: stefan.paetow.janet