Moonshot + Jisc Assent

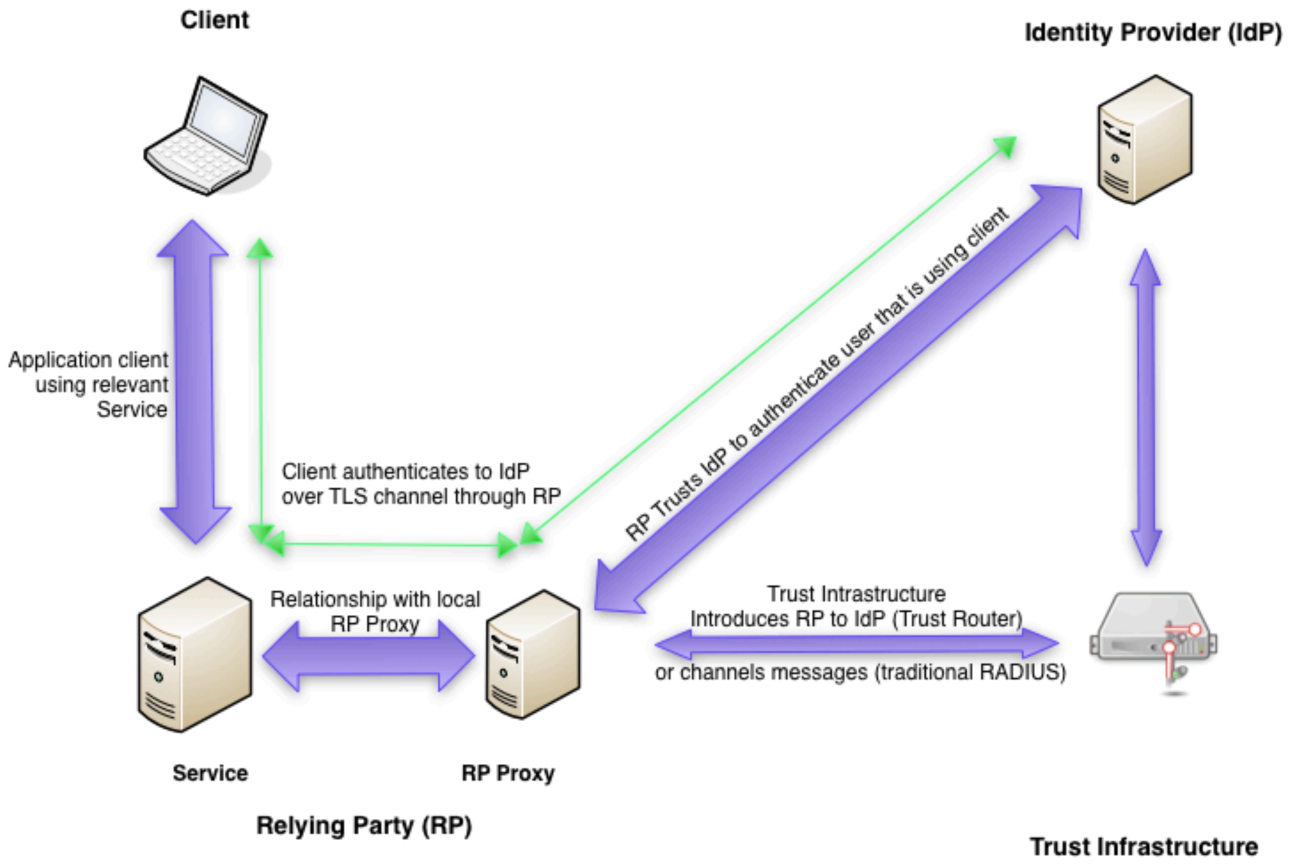
The future

Moonshot – What?

- A long-term project for Janet (now Jisc) – UK NREN
- Moonshot is a set of IETF standards
  - RFC7055, RFC7056, several drafts
- It uses proven technologies
  - RADIUS, SAML (OASIS/Shibboleth), GSSAPI (MIT)
- Designed to solve the problem of federated authentication beyond the web (ABFAB)
- It is finally here: Jisc Assent launched 25/03

Moonshot

How it works – The diagram


Client
Identity Provider (IdP)
Application client
using relevant
Service
Client authenticates to IdP
over TLS channel through RP
RP Trusts IdP to authenticate user that is using client
Relationship with local
RP Proxy
Trust Intrastructure
Introduces RP to IdP (Trust Router)
or channels messages (traditional RADIUS)
Service
RP Proxy
Relying Party (RP)
Trust Infrastructure

Moonshot

Some concepts

- EAP: Extensible Authentication Protocol
  - Runs as part of RADIUS, think of it as an envelope
    - Outside, anonymous username: “@homerealm.org”
    - Inside, real username: “bob.jones@homerealm.org”
    - Can only be opened by server for homerealm.org

- GSSAPI: Application API, designed by MIT Kerberos team
  - Moonshot uses a GSSAPI mechanism: mech_eap
    - RADIUS client that sends EAP requests over GSSAPI

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

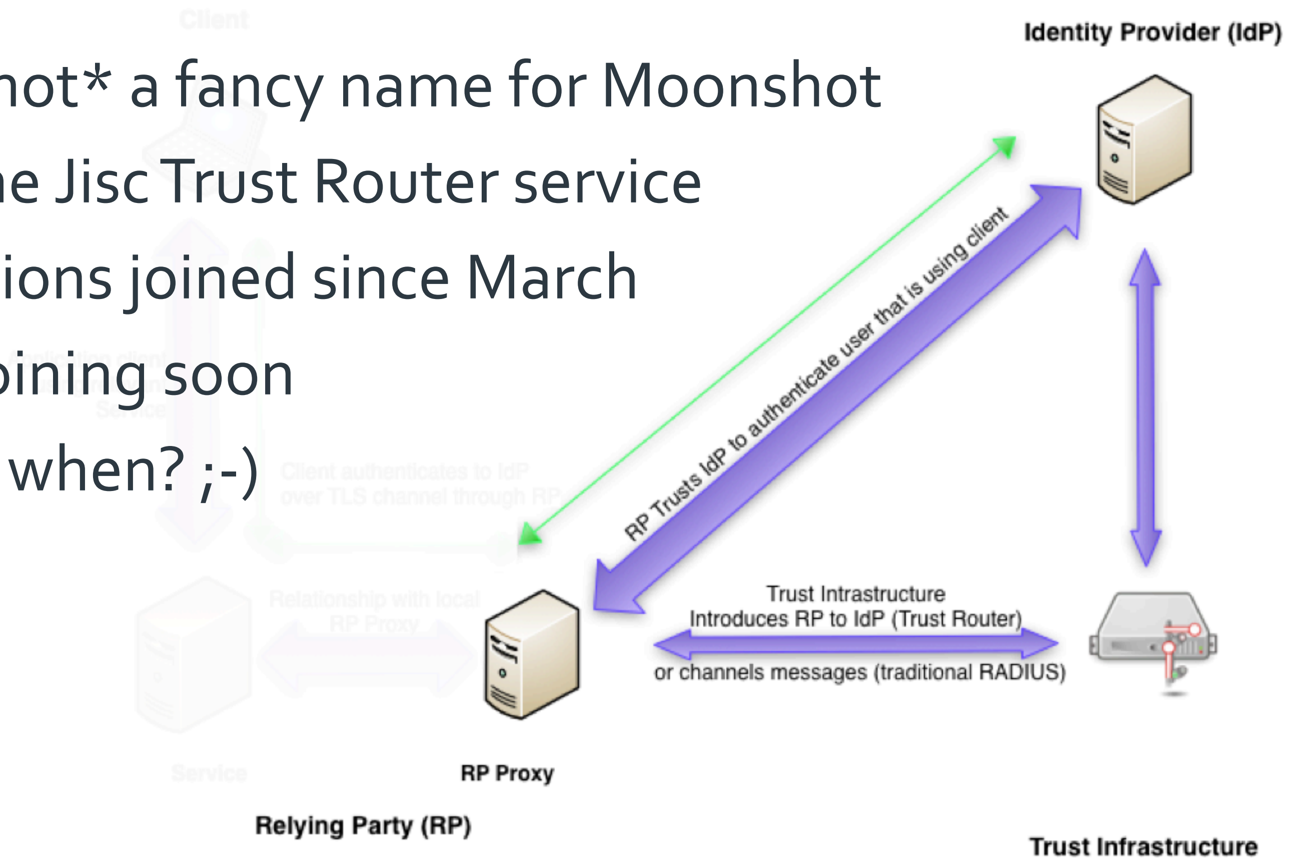
How it works (2/2)

- 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

Assent

What is Assent?

- » Assent is *not* a fancy name for Moonshot
- » Assent is the Jisc Trust Router service
- » 9 organisations joined since March
- » Diamond joining soon
- » Umbrella – when? ;-)


Client
Identity Provider (IdP)
RP Trusts IdP to authenticate user that is using client
Client authenticates to IdP over TLS channel through RP
Relationship with local RP Proxy
Trust Infrastructure
Introduces RP to IdP (Trust Router)
or channels messages (traditional RADIUS)
Service
RP Proxy
Relying Party (RP)
Trust Infrastructure

Moonshot Progress

What's happened since going live?

- The GÉANT pilot continues (next slide)
- Development + bug fixing (business as usual)
- Software support
  - gss_web: Browser plugin + Apache module done
  - OpenSSH: Making s-l-o-o-o-o-o-o-w progress
  - myProxy: Jim Basney (NCSA) confirms it works
  - NFSv4: Daniel Kouřil (CESNET) made it work
- FARR Institute (health data) ramping up for Assent

European (GÉANT) Moonshot Pilot

What's happened since?

- Pilot continues for another year
- Projects:
  - Universidad de Murcia (Openstack + Kerberos ticket forwarding with University of Kent)
  - CSC (Finland – iRODS + grid computing)
  - RÉNATER, SWITCH, REDIRIS et al (TR networks)
- Validates Trust Router routing across NRENs
- Built interest in other communities across Europe

Moonshot – The road show

What other communities?

- GRID + HPC computing
  - STFC, SAFE, CSC, EGI, OGF
- Structural biology
  - STRUBI + Diamond: Instruct/BioStructX/iNEXT/WestLife/Corbel
- Possibles:
  - Globus/GSI
  - ELIXIR
  - others…

Moonshot – Future

What do we still need?

- We identified credential delegation as being important
  - Priority for us for HPC + Grid
  - Better web access (GSSAPI over Javascript)
- CSC ran a HPC pilot (GÉANT)
  - Found it useful for new users (easier than certs!)
  - Current cert users find certs easier
- We're aware of SAFE+Moonshot (DiRAC + STFC)

Moonshot Implications

Network implications:

- Between client + service (workstation), service + RP Proxy
  - 8-15K per user AuthN request, 3 – 5 seconds
- Between RP Proxy + outside world
  - 56K per initial TID request (4x13K), 5 – 10 seconds
  - 36K per initial Trust Router AuthN request, limited by key expiry
  - 8-15K per user AuthN request, 3 – 5 seconds
- Could cache AuthN decisions on RP Proxy, but security implications apply!

What does Moonshot mean for institutions?

User implications:

- Like eduGain – Log in anywhere where it's supported
  - Could even use same credential as eduGain!
- Can log in with a known credential
  - No remembering loads of different credentials
- Can work web and non-web
- Others that haven't been thought of

What does Moonshot mean for institutions?

Security implications:

- Careful thought about user account mapping
  - Especially for industrial users, where output is owned by industrial, not user (like for other research)
- Mapping support
  - How to deal with security breaches (unlink accounts?)
  - Backward-compatible support in user office systems
    - Diamond has CAS client, but like pam_gss, web context would have access to username + password
- There may be others I don’t know of

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 (not 8.1)
  - Windows 10 in the works
- No Mac OS X yet

Moonshot
Required components

- Moonshot client (moonshot-gss-eap, moonshot-ui)
  - Windows client (Moonshot SSP)
  - Needed on client, RP Proxy, IdP
- 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

Software support

- Browsers that support multi-trip GSSAPI
  - Chrome, Firefox/Iceweasel, Internet Explorer
- OpenSSH 5.3, 5.9 (both with patch on server-side)
  - Close to getting patches approved for use by distros
- putty 0.65 (with patch)
  - Once Windows SSP stable, patch likely to be approved
- Apache 2.2
  - mod_auth_gssapi (CESNET module)
- Console access with pam_gss

Moonshot

Repo + security support

- Moonshot software is available from our repo:
  - http://repository.project-moonshot.org/rpms/centos6
- OpenSSH server software
  - On repo for Debian, RHEL is in testing
- Apache module, FreeRADIUS + putty
  - Apache module + FR will also be on our repo
  - putty is on Dropbox, as is pam_gss (PADL supplied)
- We'll keep up to date on security updates + notify where needed.

Questions

What questions have you got for us?

- Moonshot details:
  - https://wiki.moonshot.ja.net
  - My email: stefan.paetow@jisc.ac.uk