Moonshot
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
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
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
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)

» No Mac OS X yet
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
The Janet Moonshot Pilot
What did local pilot do?

» Helped define + validate RHEL/Debian documentation
» Tested mappings, RADIUS policies
» Tested other components: iRODS, SSH, OpenStack, OwnCloud
» Validated user interaction on console + remote access
  › DLS Beamline was a vital real user test – successful!
  › Demo: Moonshot + Umbrella ID with Oxford Structural Biology scientists
» Helped sell concept of Moonshot to other ESRI efforts
European (GÉANT) Moonshot Pilot

» Europe-wide pilot continues for another year
» Pilot includes:
  › Umbrella ID (joined at Diamond’s prompting)
  › University Murcia (Openstack + Kerberos ticket forwarding with University of Kent)
  › CSC (Finland – iRODS and grid computing)
  › RÉNATER, SWITCH, REDIRIS et al (TR networks)
» Validates Trust Router routing across NRENs
» Built interest in other communities across Europe
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 will be added soon

» Apache module, FreeRADIUS + putty
  › Apache module + FR will also be on our repo
  › putty will be on Dropbox, as is pam_gss

» We’ll keep up to date on security updates + notify where needed.
What does Moonshot mean for institutions?

User implications:

» Like eduGain – Log in anywhere where it’s supported
» 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
The live service: Assent

» Signed up several universities
» One HPC and a light source are joining soon
» A health data project (FARR Institute) is ramping up to use Assent
» GÉANT 4 pilots continue
Moonshot – The future
Grid world… Could Moonshot help?

» We identified credential delegation as being important
  † Priority for us

» CSC ran a HPC pilot (GÉANT)
  † Found it useful for new users (easier than certs?)
  † Current cert users find certs easier

» What else? For us this is a big step into the unknown

» We’re aware of SAFE+Moonshot

» How would you like to use it?
  † Send us use cases.
Questions?

What questions have you got for us?

» http://wiki.moonshot.ja.net/
» Stefan.paetow@jisc.ac.uk