Moonshot – An update
REFEDS 40 @ TNC 2019, Tallinn, Estonia
Moonshot – An update
What we’re going to cover

» What is Moonshot
» A retrospective
» The current state of play
» Where to next?
ABFAB – Federated access beyond web
Why do we need this Moonshot thing anyway?

» You’ve heard of eduroam
  › Federated network access through RADIUS

» You’ve heard of eduGAIN
  › Federated web access through SAML

» We have ABFAB
  › Provides for federated non-web access
  › It’s a combination of the above
ABFAB – Federated access beyond web

What is ABFAB?

» ABFAB...

› Stands for: Application Bridging for Federated Access Beyond the web

› Is a collection of 6 IETF RFCs and 1 draft
  - RFC7055, RFC7056, RFC7057
  - RFC7831, RFC7832, RFC7833

› Uses other technologies: RADIUS, SAML, GSSAPI

› Is... Moonshot
Moonshot – Looking back (1/4)

» The concept of Moonshot is a decade old!
» Proposed at “Beyond Web SSO” BOF @ TNC 2009, Málaga
» First IETF drafts, March 2010
» Briefing paper @ TNC 2010, Vilnius
Moonshot – Looking back (2/4)

» ‘Trust Router’ intro @ Internet2 Fall Members Meeting 2012
» IETF 86 Bar BOF for Trust Router, March 2013
» 18-month Production pilot, April 2013
» First IETF drafts approved, December 2013
» Production service (Jisc Assent), March 2015
» Final IETF drafts approved, May 2016
Moonshot – Looking back (3/4)

» Debian, RedHat, Windows
» Mac was... ‘missing’
» Common Internet apps tested
» Lots of pilots
  » Notable: STFC (UKRI), Diamond Light Source, CSC (Finland), University of Kent and University of Murcia
Moonshot – Looking back (4/4)

» Wiki geared to systems admins (needs reworking)

» No test network – BIG barrier to adoption
  › Requirement to sign up to full Assent service
  › If you can’t show your management, how can you get sign-off?

» Features not available:
  › No non-X UI
  › No encryption of text-only ID management (big barrier)
Moonshot – Where we are today (1/4)

» New features being added:
  › Non-X UI client
  › Gnome keyring support in non-X
  › ID management encryption in non-X without keyring
  › Removal of Shibboleth SP requirement
    - OpenSAML libraries still needed

» You want a new feature? Ask for it!
Moonshot – Where we are today (2/4)

» Latest versions of:
  › Debian, RedHat, Windows, macOS (MVP)

» Raspberry Pi support
  › Raspbian, Alpine

» Basic Docker images
  › We actively use these for CI
Moonshot – Where we are today (3/4)

» Trying new things when requested
  › “Does this work with Moonshot?”
  › “Let’s find out!”

» AARC BPA-compliance
  › Includes ‘proxying’ support in Moonshot clients

» Actively trying vendors to adopt proper GSSAPI standards
  › Nomachine is first vendor to actively bake Moonshot support into product
Moonshot – Where we are today (4/4)

» Moonshot is in H2020 projects
  › CALIPSOplus actively demands Moonshot
  › PaNOSC, LEAPS rely on CALIPSOplus
» UKRI (IRIS) lists Moonshot as option (in progress)
» Paul Scherrer Institut (Switzerland)
  › SLS MX beamline (40% of SLS science) moonshotted
» EGI potentially interested in EGI-Checkin + Moonshot
» AARnet a possible candidate
Moonshot – Where we are going (1/2)

» Continual package improvements
  › Why have manual steps if RPM or DEB can do it?
» We’re moving on with infrastructure
  › Soon no longer ‘VM’ based
  › Moving to cloud for operations
» Everyone loves Docker
  › Let’s build Docker images that do most of the heavy lifting
  › Click, deploy, connect, presto!
Moonshot – Where we are going (2/2)

» Work with eduroam deployers
  › If you use FR 3.x, why not plug in Moonshot support?

» IdP-as-a-service
  › Can use Shibboleth-to-RADIUS component?
  › Jisc Liberate had Assent support scheduled but... 😐
Moonshot – Challenges (1/2)

» Lack of platform buy-in
  › Apple (next slide)
  › Microsoft (client is not ours)
  › Linux (LTS rules don’t allow new feature rollout)

» Lack of facility buy-in
  › YAP – Yet Another Protocol
    - Needs system admins + management buy-in
  › No incentive to deploy Moonshot (_runner + _runner_)
Moonshot – Challenges (2/2)

» Apple
  » Continually moving target
  » Tightening ‘sandboxing’ reduces ability to Moonshot
  » Will ‘Sign in with Apple’ kill Moonshot on Mac? 🤔

» OIDC/OAuth2
  » Science is moving on! 🎓
  » A lot of non-browser SSO is OIDC-token-based
  » Social conditioning to only trust web browser
Moonshot – The future

» Still a good technology
» Can be deployed for IoT login (FRuIT project proven)
» Does not necessarily *require* Trust Router (would be nice though)
» Interesting cases to explore
  › eduroam discovery via Moonshot (instead of DNS)?
  › eduroam proxy lookup instead of visited organisation?
Sooo... Moonshot
Where can I find more info?

» Moonshot Wiki:
  › https://wiki.moonshot.ja.net/

» Email me or Alex:
  › stefan.paetow@jisc.ac.uk
  › alex.perez-mendez@jisc.ac.uk

» Want to test a test system? Get in touch!