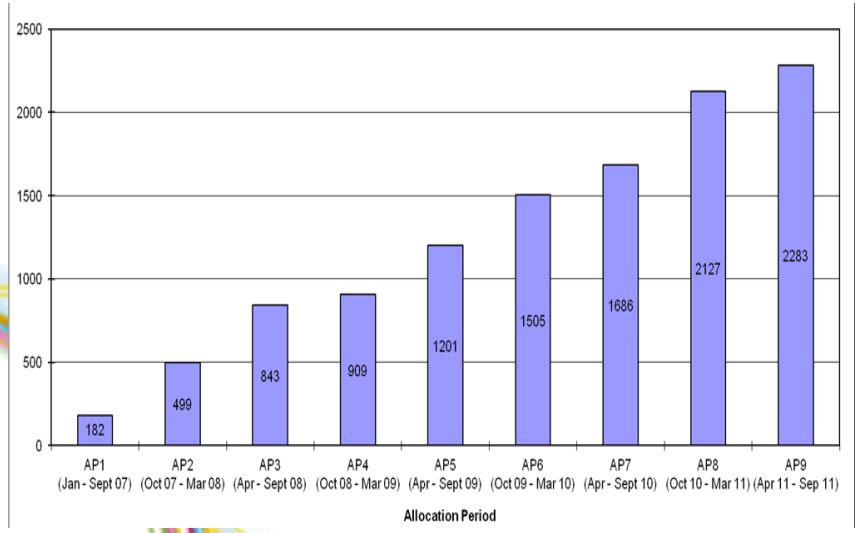
Moonshot @ Diamond

Diamond, Umbrella + Federated access

Jan 2011 - 2012, DLS had 1,726 experimental visits + 4,976 external experimenters, of which 1,976 were unique. Numbers are growing!

Umbrella:

- Web-based authentication system based on Shibboleth SSO
- Rolling out to several European physics facilities (PSI, ILL, ESRF, ISIS)



Federated access

1. Facilities join federation, agree attributes + identifiers common/safe to use (political, data protection, etc.) at all facilities

2. Account creation – Either:
   - Use common/shared system (central, not always ideal or acceptable)
   - Auto-create for persons from facilities in federation (easier, but less secure)
   - Link local account to identifier from facilities in federation (two-step process, but better security) – **DLS preference!**

3. Once account/link established, user can log in with home ID, local systems accept user under local account

Moonshot + Umbrella + eduroam = Win

- Built a proof-of-concept that:
  - Allows interactive/console, SSH, WWW login with DLS FedId, eduroam ID or Umbrella ID using Moonshot
  - Has been tested with virtual beam-line, provides access to user's home directory
- Demonstrated PoC in Berlin (eduroam) + Barcelona (Umbrella) to PaNdata
  - Response was cautiously positive

Diamond Proof of Concept

- Set up a set of test VMs
  - RADIUS server VM
  - Two different eduroam ‘institutions’ (uwa + camford)
  - ‘Beamline console’ with Moonshot libraries, SSH + pam_gss installed
  - SAMBA 4 server – 100% Active Directory compatible
  - Real Umbrella Shibboleth server

- Set up ‘glue’ database that maps local users to eduroam CUI + Umbrella EAAHash

- Set up local user accounts on the ‘beamline console’

Moonshot service implementation

Console login access – Small change in PAM stack:

- Insert pam_gss before password-auth / system-auth in gdm-password
- Use ‘try_first_pass’ not ‘use_first_pass’ in password-auth / system-auth for ‘auth’ only.

SSH – pam_gss appears to be not compatible with SSH’s PAM stack

- Recommended to use GSSAPI mechanism
    - Needs Moonshot version of OpenSSH
- Set GSSAPI* in sshd_config to ‘yes’, PasswordAuthentication to ‘no’
- Run on alternate port perhaps...

On clients connecting to SSH server:

- Minimum: Moonshot software (Moonshot OpenSSH **optional**)
- ssh_config: GSSAPIAuthentication, GSSAPIKeyExchange both ‘yes’

Moonshot web implementation

- Web access @ DLS continues to use CAS as authentication server
- DLS helped JASIG fix their RADIUS support, to be released in CAS 4.0.0
- DLS also wrote Moonshot connector for CAS 3.x and 4.x
  - Allows us to log via the same RADIUS mechanism as with console
  - Advantage: One RADIUS to rule them all
  - Disadvantage: ~1 auth failure per Umbrella login (no EAP negotiation mechanism)

What's next?

- Technically, Umbrella could roll out 'tomorrow'

- eduroam support relies on Chargeable-User-Identity (CUI) returned by home sites
  - CUI 'recommended' in eduroam spec, Janet has a blog for it
  - CUI not mandatory because of platform interop questions (NPS etc)
  - Janet is aware that we need CUI support

Questions?