Moonshot at Diamond

Implementing federated authentication with Moonshot at the Diamond Light Source

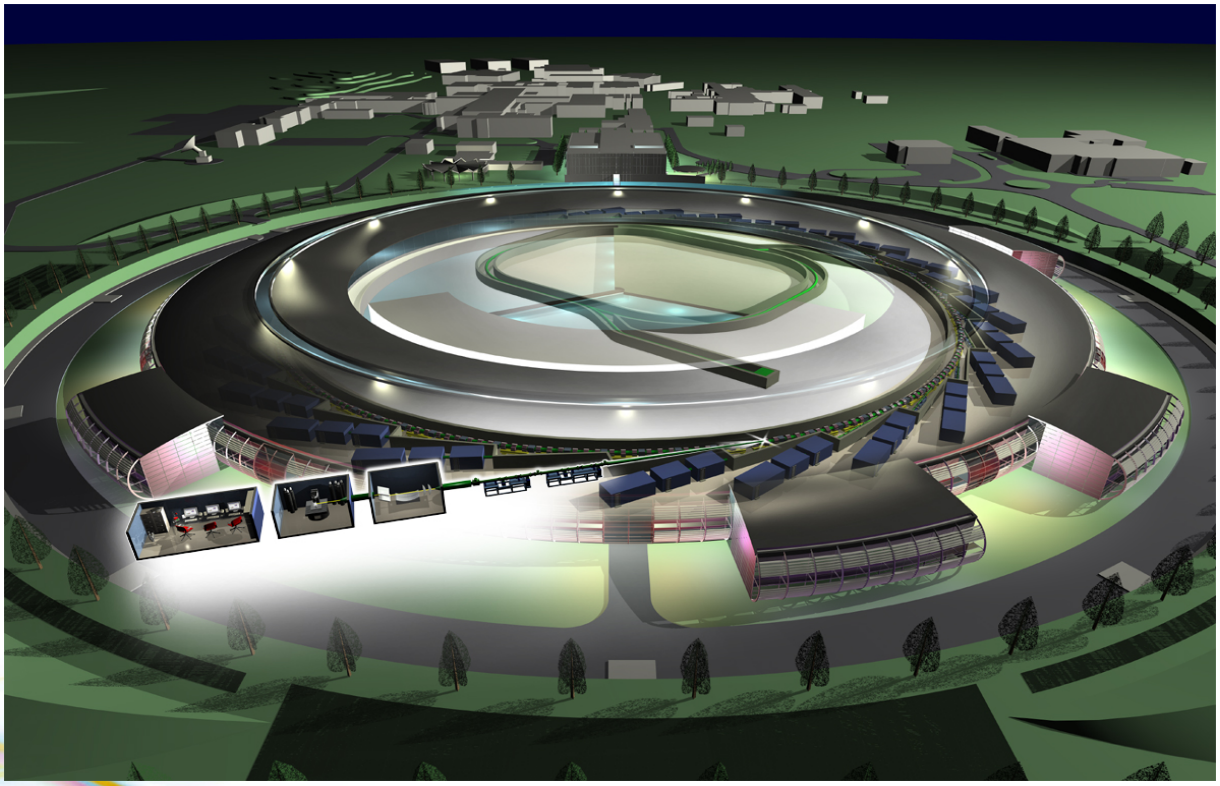
Janet Networkshop42, University of Leeds, 2 April 2014

What is... Diamond?

What is... Diamond?

- The largest scientific investment in the UK for 45 years ~(£263M + £120M + £66M) in three phases;
- A source of extremely intense light, particularly X-rays and can be thought of as a huge microscope
- Funded by our shareholders – UK Government through STFC (86%) and the Wellcome Trust (14%)
- Free at point of use to UK academic users
- Increasing direct contributions to UK industry

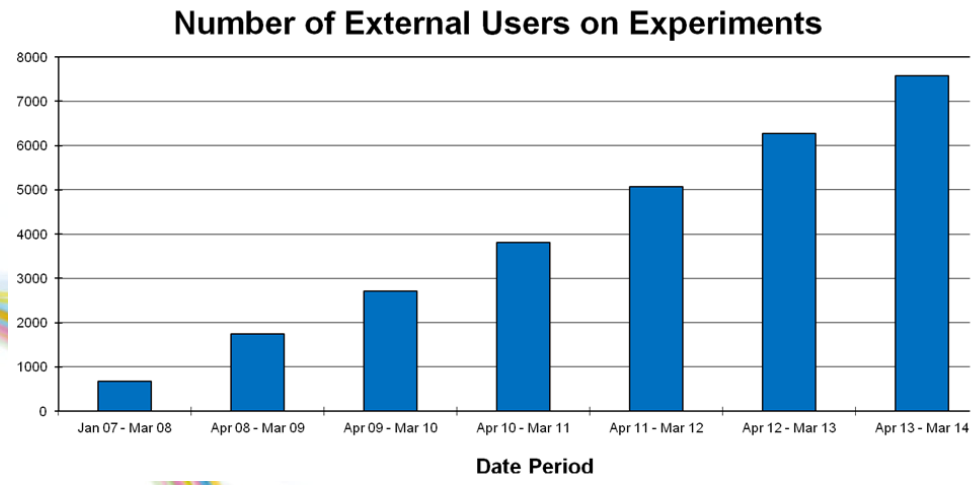
How does Diamond work?



Diamond User + Data Figures

In the last six months, DLS had >3,800 external experimenters, of which 1,822 were unique, and ~1,200 never even set foot inside the facility.

As of March 2014, 1 petabyte of experimental data has been generated, weekly volume ~20 million files (>22TB), growing exponentially



Diamond + PaNdata

Number of Users shared between facilities																	
	BER II	BESSY II	DESY	DLS	ELETTRA	ESRF	ILL	ISIS	LLB	SINQ	SLS	SOLEIL	FRM-II	ANKA	neutron	photon	all
BER II	850	80	68	25	18	128	261	141	67	76	12	14	111	5	375	244	850
BESSY II	80	2306	238	45	134	399	67	33	31	26	149	93	42	31	175	758	2306
DESY	68	238	3563	88	121	735	194	91	55	44	155	130	103	43	356	1105	3563
DLS	25	45	88	3494	72	739	213	336	35	18	145	149	20	12	441	967	3494
ELETTRA	18	134	121	72	2731	455	85	43	23	4	66	316	9	20	145	839	2731
ESRF	128	399	735	739	455	10728	886	406	235	92	600	1069	144	80	1303	3256	10728
ILL	261	67	194	213	85	886	4338	741	343	229	69	176	349	10	1450	1246	4338
ISIS	141	33	91	336	43	406	741	2755	120	119	43	52	155	5	908	716	2755
LLB	67	31	55	35	23	235	343	120	1348	34	12	131	92	3	425	359	1348
SINQ	76	26	44	18	4	92	229	119	34	726	96	9	97	0	334	210	726
SLS	12	149	155	145	66	600	69	43	12	96	2424	182	18	18	169	923	2424
SOLEIL	14	93	130	149	316	1069	176	52	131	9	182	3656	14	26	299	1460	3656
FRM-II	111	42	103	20	9	144	349	155	92	97	18	14	1087	5	494	255	1087
ANKA	5	31	43	12	20	80	10	5	3	0	18	26	5	452	19	144	452
neutron	850	175	356	441	145	1303	4338	2755	1348	726	169	299	1087	19	7117	2350	8852
photon	244	2306	3563	3494	2731	10728	1246	716	359	210	2424	3656	255	452	4517	19902	24154
all	850	2306	3563	3494	2731	10728	4338	2755	1348	726	2424	3656	1087	452	8624	19242	30873

Diamond + PaNdata

- PaNdata = **P**hoton **a**nd **N**eutron **data** infrastructure
- European Union-supported project (Framework Programme 7)
- Brings together 13 major EU photon + neutron laboratories
- Develops common data infrastructure, includes federated AIM

PaNdata + Umbrella ID

- Shibboleth chosen to be common service: Umbrella ID
- Shared between facilities
- Umbrella ID user identity linked to a local account at facilities
- Disadvantage: Web only
- Umbrella ID is joining GÉANT initiative for Moonshot
    - Also linking Umbrella ID and eduGAIN

Moonshot

- Janet-led initiative
- As of late 2013, IETF approved RFC 7055-7057
- Combines proven RADIUS AAA with GSS API and SAML flexibility + richness
- Now in pilot phase
- Trust router network has two IdPs (Janet + Uni Cardiff)
    - DLS hopes to join as third IdP soon

How secure is Moonshot?

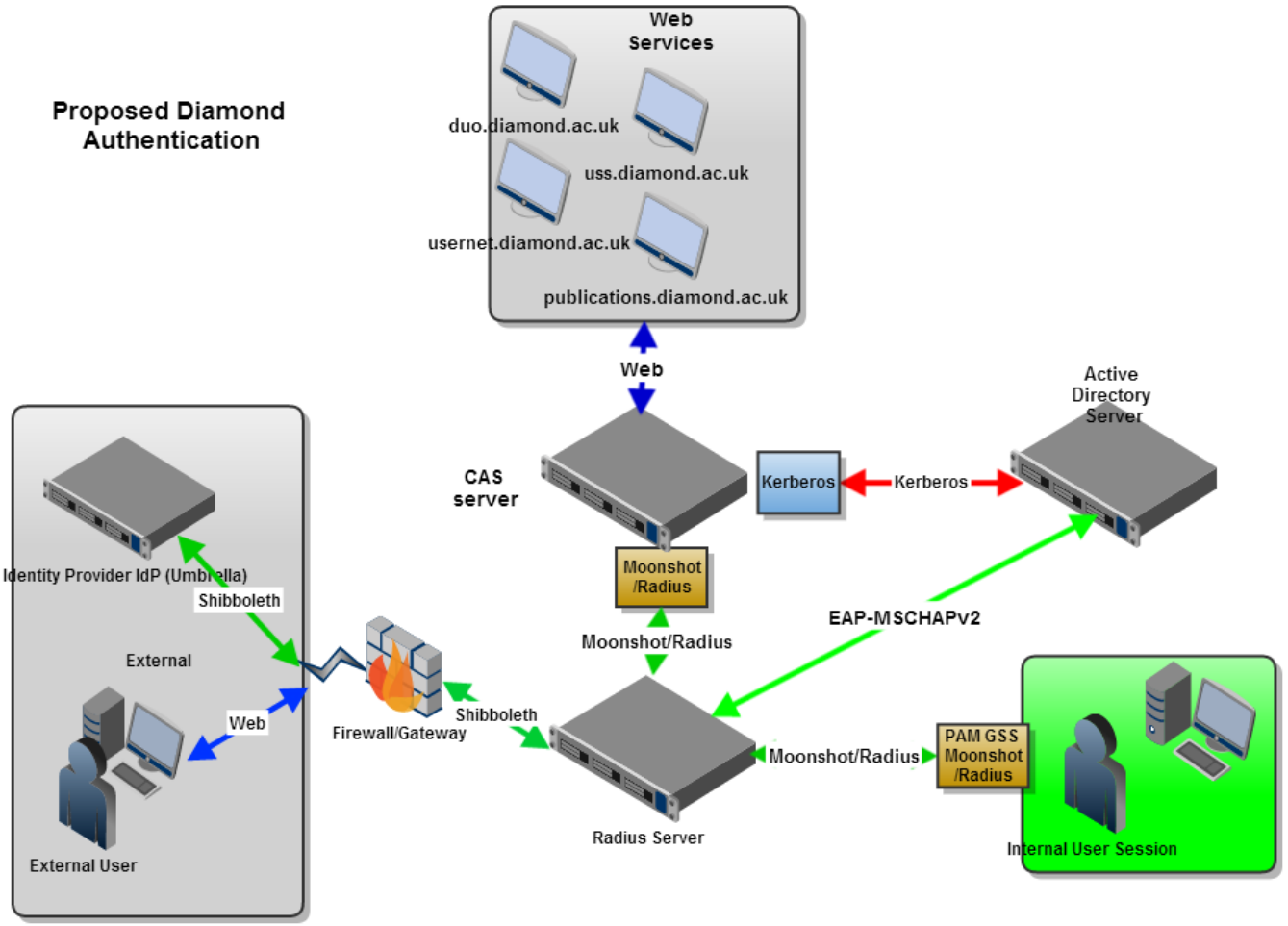
- Moonshot itself uses RADSEC + EAP-TTLS authentication
  - Trust router is P2P, includes secure tunnelling between IdP + SP

- Client authentication uses proven GSS API
  - SSH uses GSS-API into Moonshot
    - OpenSSH + putty patches going upstream
  - Web access to use SPNEGO + Moonshot GSS components
    - Alternative: Use Jasig CAS ABFAB authenticator (as secure as server is)
  - Console access uses pam_gss, as secure as workstation is

Moonshot identity

- RADIUS uses username@realm for authentication
  - Moonshot continues with that format
- SSH access through GSS-API authentication
  - Moonshot UI (in X) or file-based user credentials
  - Passwords stored in GPG keyring
- Web access with SPNEGO (using Moonshot UI), Javascript API or username@realm + password
- Console access (via PAM) with username@realm format and password

Diamond + Moonshot



Diamond + Moonshot

- Moonshot gives users login flexibility
- Users only need to remember one set of credentials (their linked one)
- Users can link DLS account (FedId) with home credentials
  - Umbrella ID is currently supported
  - eduroam tested, subject to support by home organisations
- Log into systems with credentials of their choice, system knows their FedId
- Can access local resources as much FedId permissions allows them to

Diamond's Moonshot progress

- Connected Moonshot PoC with eduroam authentication (June '13)
- Added Umbrella as additional authentication source to PoC (late Aug '13)
- Published Jasig CAS ABFAB authenticator on Maven Central (Nov '13)
- Built Shibboleth ECP client together with DARIAH-DE (Dec '13/Jan '14)
  - Used indirectly in new iCat Shib2Local authenticator
- Launched pilot beamline with Moonshot + Umbrella using above (Mar '14)
- To join trust router network soon (Apr/May '14?)

Demo + Questions?