janet

Moonshot

Josh Howlett

5 December 2012

Janet – the UK's research & education network

janet

- Janet is a not-for-profit company that manages the operation and development of its service portfolio on behalf of the JISC for the UK FE/HE Funding Councils
- Janet's service portfolio includes the high speed network, and other services that build on it
  - This includes a portfolio of Access & Identity Management (AIM) services, and related service development activity
- Janet has approximately 18 million eligible users, from UK schools, HE, FE and ACL programmes

Moonshot

Use Cases

Use cases

janet

Lets dive straight in and look at some use cases:

- That have no current deployable federated solution, apart from Moonshot
- Have a user experience that can be significantly improved by Moonshot
- Have existing deployment models whose cost and effort can be reduced by Moonshot

This is just a small sample, to illustrate the range of possibilities…

Cancer Research UK

Cancer Research UK is the world's leading charity dedicated to beating cancer through research.

- The institutes form ad hoc relationships to collaborate for research purposes, but when the need arises to share data and documents, each institute can only authenticate within their own organisation.

"Moonshot is a valuable enabler for Cancer Research across the UK. It will make collaboration systems easy to build internally so that we can quickly share large data sets between institutes, without complicating the management of that system."

Peter Maccallum, Head of IT & Scientific Computing, CRUK Cambridge Research Institute

Moonshot and… Federated Sharing of Data

janet

Many organisations collaborate with others, wanting to share data and documents:

- E.g. Provision of access to remote file systems (SAMBA / CIFS / NFS)
- Today, users' credentials must be managed by the provider

Using Moonshot, authentication happens at user's home organisation – provider does not manage and 'see' the credentials

Moonshot and… Cloud Services

janet

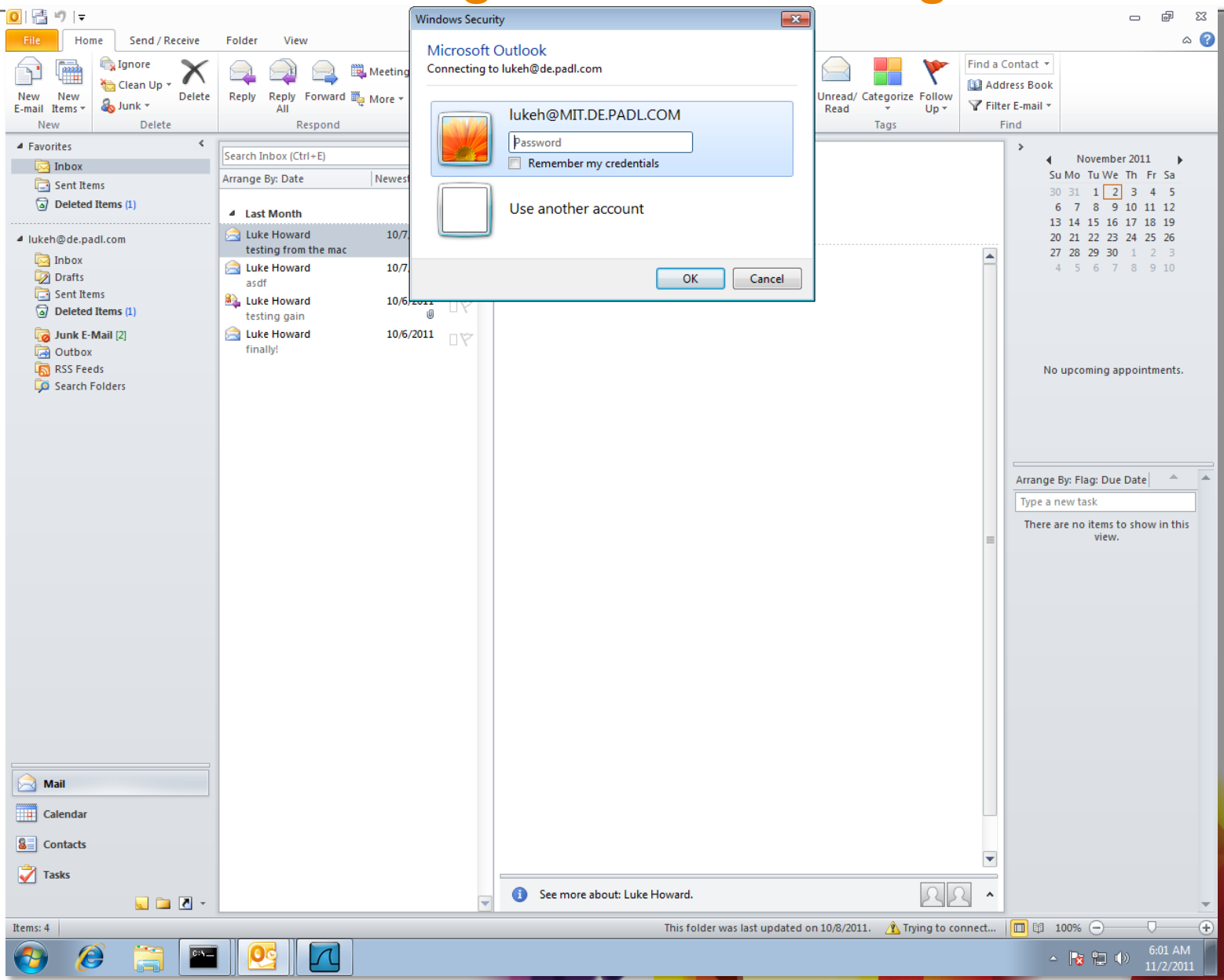
Many organisations are outsourcing services to the cloud, or delivering services in the cloud

- For example: Exchange in the cloud
- Today, user's credentials must be supplied to the provider
  - E.g. Using directory synchronization technologies
- SAML authentication an option for some, but not all, and not all clients (e.g. Microsoft Lync client)

Using Moonshot, authentication happens at user's home organisation – provider does not manage and 'see' the credentials

e.g. Outlook connecting to hosted Exchange

janet



Diamond Light Source

The UK's national synchrotron facility

- Piloting Moonshot within the PANDATA project, which supports a community of 30,000 scientists from 100s of organisations at 20+ photon and neutron facilities

- Federated access needed to physical consoles in person, or remotely using SSH

"Moonshot has thought beyond websites, and looked at what is really required in authentication – right down to the point when you open your laptop to begin work."

Bill Pulford, Head of DASC, Diamond Light Source

Moonshot and… Federated SSH

janet

Organisations with compute clusters typically:

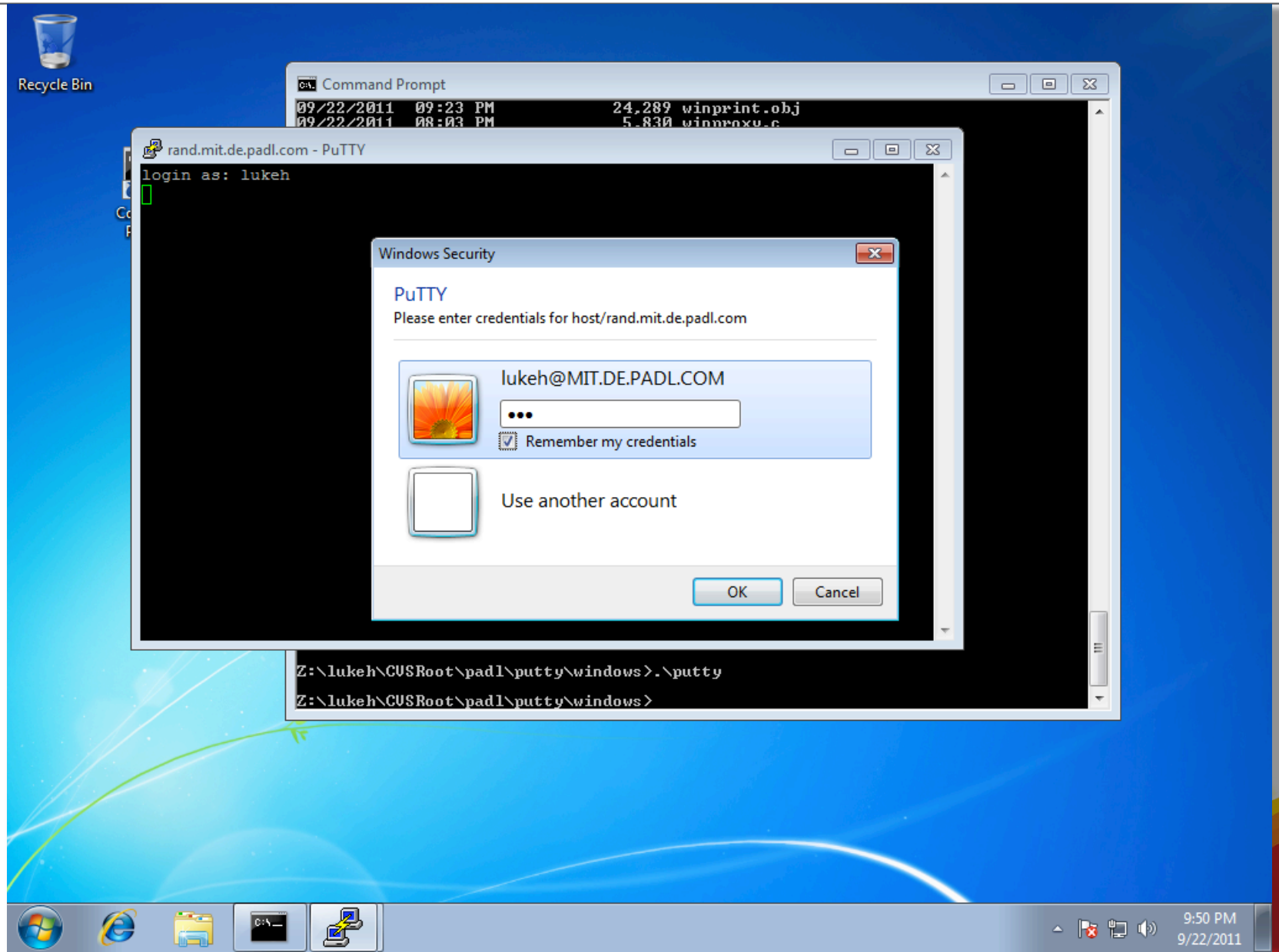
- Allow access through SSH
- Have a community of users, some internal some external
- Have to manage the credentials of all users

Using Moonshot for SSH access:

- Authentication happens at user's home organisation – no credentials to manage at service!
- Various options possible for mapping users to accounts

e.g. PuTTY connecting to Linux OpenSSH

janet



Moonshot and… Federated Desktop Sign-in

janet

Some organisations want to enable manageable desktop sign-in for external users

- Seconded personnel, visitors, contracts, etc;
- Or beyond – e.g. public sector desktops that should allow local government users, police users, fire users, health workers, social services users, etc

Highly challenging using contemporary technology

Moonshot integrates directly into Windows and Linux desktop sign-on

Other tested scenarios

janet

For example… (these are tested, working examples)

OpenLDAP client → OpenLDAP server (GSS)

OpenLDAP client (GSS) → Windows Active Directory (SSPI)

Firefox → Apache (GSS)

Internet Explorer → IIS (SSPI)

MyProxy client → MyProxy server (SASL)

Adium → Jabberd (SASL)

Moonshot

Introducing Moonshot

janet

Moonshot's Goals

Lower the barriers to collaboration within the Janet community

Reduce the cost and time to create new services

Drive down operational costs for both Janet and our community

janet

How?

By enabling our customers to **Federate Anything** & **Everything, Easily**

By enable communities to **manage themselves**

By **unifying** the disparate trust technologies in use today

Moonshot Technology

janet

Moonshot builds on deployed, proven technology…

- Strong authentication used by eduroam (EAP/RADIUS)
- Strong authorisation used by UK federation (SAML)
- Strong service/application integration used by many major applications (operating system security APIs)

Standardisation approaching completion within the Internet Engineering Task Force (IETF)

- Moonshot is Janet's open source implementation

Moonshot's Flexibility

janet

Moonshot enables:

- Federated authentication to virtual any network-connected system, application, or service
- Virtually any deployment model (centralised, distributed, cloud)
- The use of almost any kind of authentication credential

A unified trust & identity infrastructure, capable of satisfying virtually any security requirement

janet

Moonshot

Benefits of Moonshot

Federate Anything & Everything, Easily

janet

Moonshot integrates with OS level security APIs (GSS-API / SSP / SASL)

- Proven, deployed technology already in use by many applications within your organisation
  - Many applications already support Moonshot with little or no modification
- (Kerberos is a well-known GSS-API mechanism)

Easy to Deploy

janet

Many organisations already have the necessary infrastructure

- A RADIUS server (you may have already for eduroam)
- A SAML server (you may have already for an AAI federation)

If so

- You already have the technology and skills in place

Easy to Manage

janet

Communities set up and managed by those closest to them – themselves!

- Saves on administrative overhead **everywhere**
- Less specific technical technical change required at each IdP/ Service to support individual communities
- Policies can be targeted for the specific community
- Easier and more intuitive for users

How?

Easy to Manage

janet

Community management portal

- Communities create and manage themselves in the portal
- Easily managed list of organisations (and/or specific users) that are a part of that community and have agreed to its policies
- Services belong to particular communities
- Authorisation can happen based on community membership (amongst the other "usual" things).
- Community membership can be used to enable cross organisational authorisation ("virtual organisations")

janet

Moonshot Briefing

Deploying Moonshot - Requirements

Requirements

janet

So what's needed to "do" Moonshot?

There are 3 main roles in Moonshot:

- Identity Provider
- Relying Party (Service)
- User

Requirements – Identity Provider & User

janet

At the home organisation:

- An existing identity store (e.g. LDAP)
- RADIUS Server
- SAML Server

On the user's device:

- Moonshot libraries
  - MSIs on Windows, RPMs/Debs on Linux, installer on Mac
- A way of choosing the identity
  - Moonshot Identity Selector / Windows Credential Manager

Requirements – Relying Party

janet

At the service:

- RADIUS Server
- Moonshot libraries
  - MSIs on Windows, RPMs/Debs on Linux, installer on Mac
- Service configured to use GSS/SSP/SASL authentication

janet

Moonshot Briefing

Janet's Moonshot Pilot Service

Moonshot Pilot Service

janet

18 month pilot

- Begins April 2013
- All technology production ready and in place
- Portal for managing communities available
- Support available for participants available

Main aims:

- Allows Janet to pilot the service and support offerings
- Allows community to pilot Moonshot with a stable backend infrastructure and with support available

Roadmap

janet

Milestone	Date
Management Portal Specification complete	October 2012
Windows SSP public beta available	November 2012
Introduction to Moonshot Webinar	Today
Identity Selector v1.0 available	December 2012
Windows SSP v1.0 available	January 2013
Trust Router Public beta available	January 2013
Moonshot Implementation Training Course Pilot	February 2013
Trust Router v1.0 available	March 2013
Moonshot Implementation Training Course	March 2013
Service Pilot begins	April 2013

Moonshot

Finally

janet

A Quick Recap

Standardised **next-gen** identity & trust technology

Building on **proven, deployed technologies**

Cross-platform implementation

Communities **manage themselves**

Easy to **deploy** and **use**

janet

A Quick Recap

Federate

Anything & Everything

Easily

Further Information

janet

Moonshot Community website:

- https://community.ja.net/groups/moonshot

Software:

- https://community.ja.net/groups/moonshot/article/accessing-moonshot-repository

Standards:

- https://tools.ietf.org/wg/abfab

janet

Moonshot

Q & A

THANK YOU

Janet, Lumen House
Library Avenue, Harwell Oxford
Didcot, Oxfordshire
t: +44 (0) 1235 822200
f: +44 (0) 1235 822399
e: service@ja.net