

The safe share project

John Chapman, Deputy head, information security, Jisc

- **What:** a pilot project enabling the **secure exchange of data** collected by Government and the NHS **using an encrypted overlay over the Janet network** to facilitate appropriate analysis between project sites
- AND reusing existing services to increase authentication for researchers
- **Why:** easier, secure access to research data to further knowledge of diseases and ill health to improve medical treatments in the long-term
- **When:** running from **November 2014 – March 2017**

Background

- Substantial investment in medical and administrative data research to generate benefits to society from the appropriate analysis of data collected by Government and the NHS
- E.g. to further knowledge e.g. of disease and ill health to improve medical treatments

Challenges

- Health data, and other routinely collected data on people's lives, are very personal and sensitive
- Significant numbers of ethical, consensual and practical hurdles to making appropriate use of the sensitive data for research

Drivers

- Requirement for connectivity to move and access electronic health data securely
- Challenge to give public confidence that data is appropriately protected
- Provide economies of scale in secure connectivity

The safe share project

- Jisc management and funding of £960k to pilot potential solutions with the aim of developing a service in 2016/17

University of Bristol
Cardiff University
University of Edinburgh
Francis Crick Institute
University of Leeds
UCL
University of Manchester
University of Oxford
University of St Andrews
University of Southampton
Swansea University



The Administrative Data Research Network

The Farr Institute

The MRC Medical Bioinformatics initiative

Authentication, Authorisation and Accounting Infrastructure (AAAI)

Use Cases:

- HeRC, N8 HPC – access between facilities using home institution credentials
- eMedLab – partners will be able to use a common AAAI to access this new system (for analysis of for instance human genome data, medical images, clinical, psychological and social data)
- Swansea University Health Informatics Group – investigating Moonshot as an authentication mechanism to allow use of home institution credentials
- University of Oxford: to enable researchers to use home institution credentials for authentication to request access to datasets for studies e.g. into dementia

- » AAAI project is using Assent - Allowing you to effectively manage and control access to a wide range of web and non-web services and applications

About Assent

- » Using Assent gives your staff and partners access to a wide range of services including cloud infrastructures, high performance computing, grid computing and commonly deployed services such as email, file store, remote access and instant messaging.
- » Assent uses the technology developed through our [Moonshot project](#) to enable single-sign on capability within, across and between organisations, where secure communication is ensured. Approved now as an international standard.
- » Assent extends the range of applications and services that can consume federated identity and improves the security of your services by controlling access to resources. It builds on existing RADIUS and SAML based technologies that underpin eduroam and the UK Access Management Federation services.

HPC Pilot:

- Leeds deployed Moonshot infrastructure, Manchester deploying soon – then testing use of Assent to log in to N8 facility.

Swansea University:

- Looking at the use of Assent as part of the Open Stack infrastructure for the Cloud Infrastructure for Microbial Genomics (CLIMB) project with Universities of Cardiff, Birmingham and Warwick. Work recently completed on providing compatibility between Moonshot and Centos7 meaning development work can now start with CLIMB – planning an AAAI workshop in July.

eMedLab:

- Technical workshop in November to investigate requirements.
- eMedLab is working to get into a production-ready state this year and will then look to pilot use of Assent.

University of Oxford:

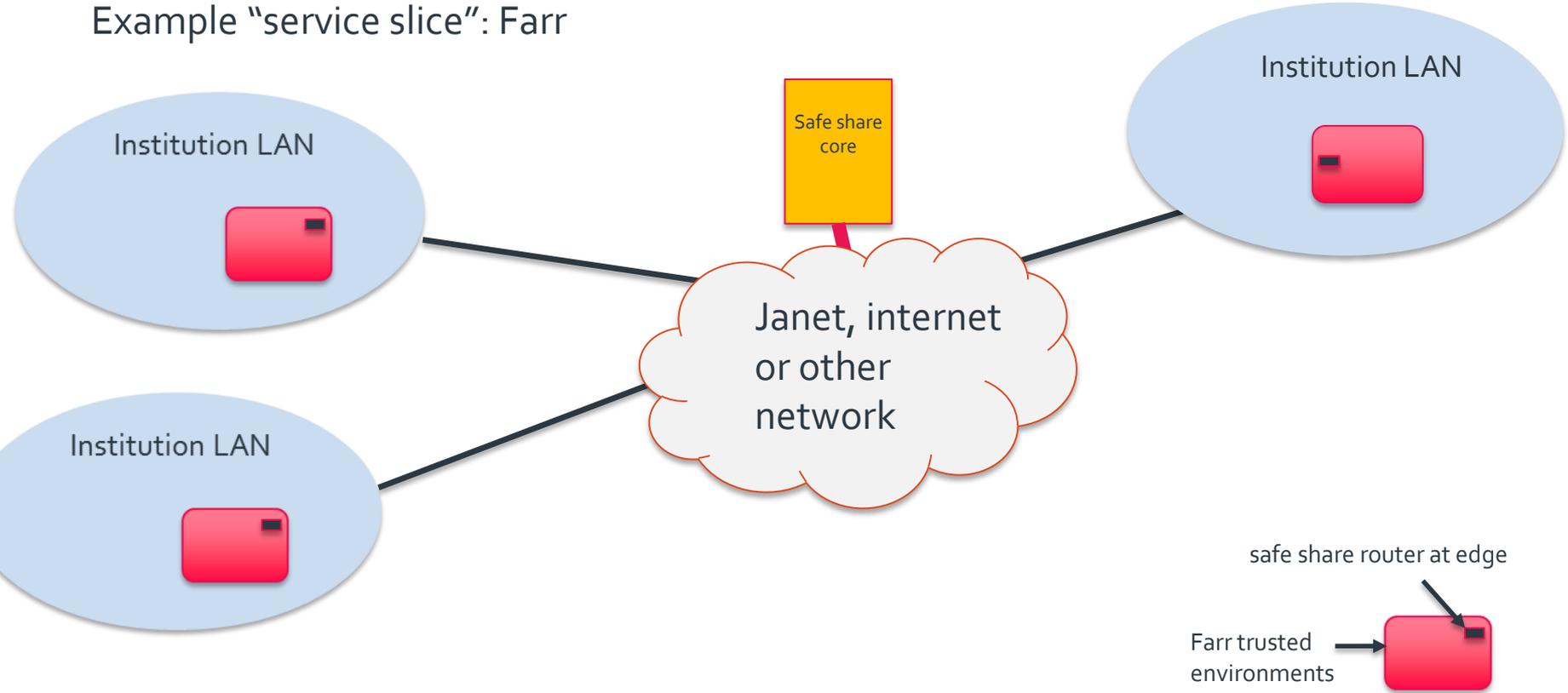
- Planning to learn from the other pilots first before applying a solution to a dementia project

Secure connectivity with a higher assurance network (HAN)

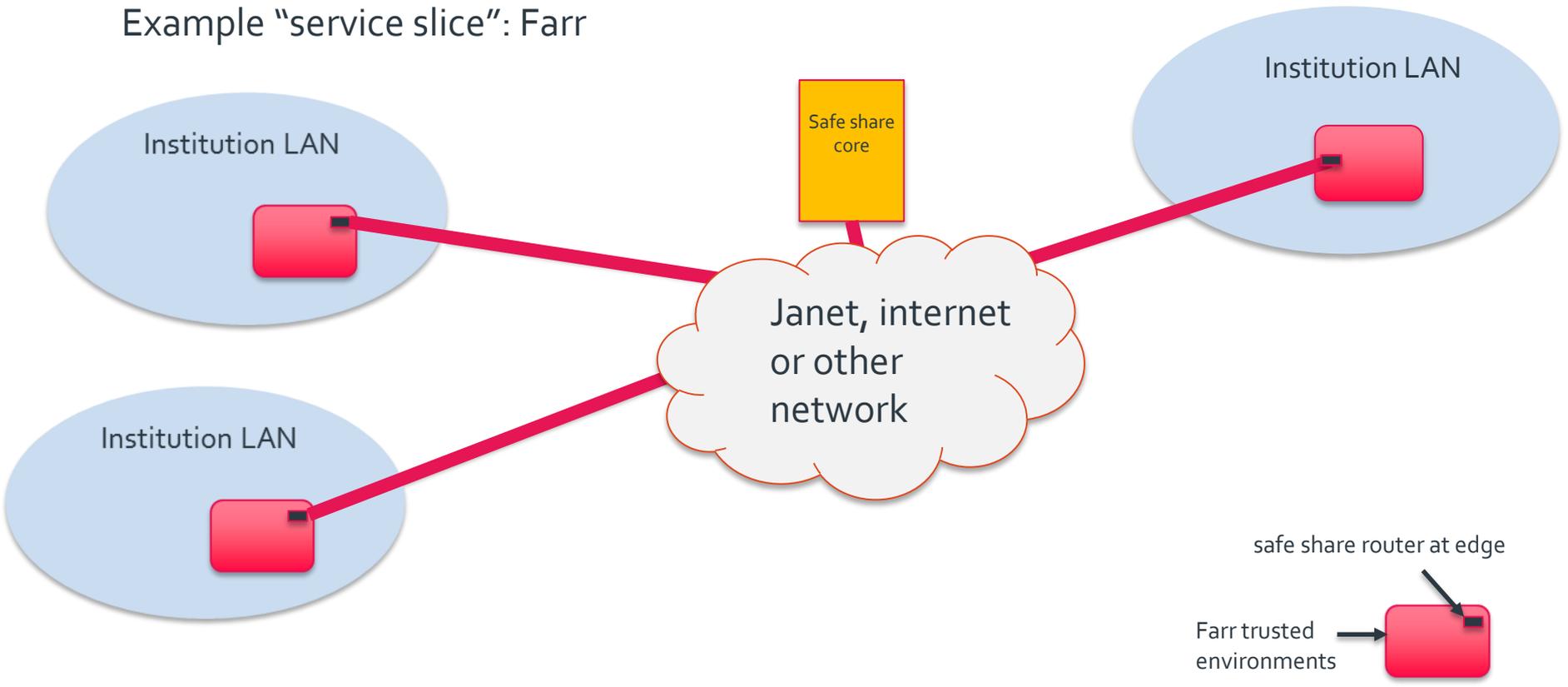
Use Cases:

- Inter-Farr – initial trial between 2 Farr facilities
- Intra-Farr – to support the ALSPAC project between Swansea and Bristol
- ADRC – connectivity between accredited secure rooms that can be connected to ADRC data centres for remote working
- PSN – extending the reach of the Public Services Network

Example "service slice": Farr



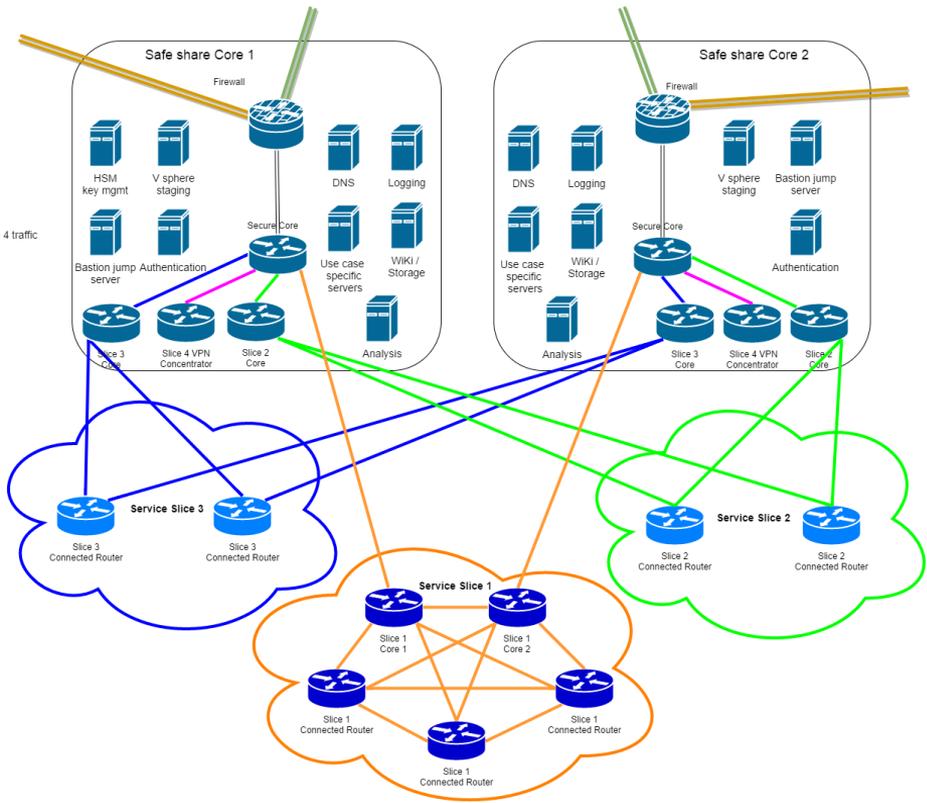
Example "service slice": Farr



The safe share project: HAN design overview

Safe share design principles

- 10 Gbps connection to Janet
 - Other external connectivity
 - Separate copper connection to firewall per service slice
 - Service slice 1 traffic
 - Service slice 2 traffic
 - Service slice 3 traffic
 - VPN Concentrator service slice 4 traffic
- 1 Gbps IPsec capable router
 100 Mbps IPsec capable router



- Safe share routers supplied to St Andrews, Southampton, Cardiff, Swansea and Manchester Universities
- Testing to start soon
- Public Services Network
- Preparing for ISO27001 and Official accreditation

- Enabling the **secure exchange of data** collected by Government and the NHS using **encrypted overlay over the Janet network** to facilitate appropriate analysis between project sites
- Working together to **further knowledge of diseases and ill health to improve medical treatments in the long-term**
- Running from **November 2014 – March 2017**
- Find out more:

<https://jisc.ac.uk/rd/projects/safe-share>

<https://community.jisc.ac.uk/groups/safe-share-project>

[#jiscsafeshare](#)