Project Moonshot

Networkshop 39

University of Hertfordshire

13 April 2011

Josh Howlett, Strategic Projects Leader, JANET(UK)

Contents

- Motivation & goals
- Use-cases
- Technology overview
- Software status
- Standardisation status

Motivation

- Multiple deployed trust & identity technologies
  - RADIUS / eduroam
  - SAML-based federation
  - Grid
  - X.590 certificates
  - Kerberos
- Results in substantial overall system complexity for consumers of these technologies.
- Can we use a single technology to satisfy *all* trust & identity requirements?

Use-case 1: Out-sourcing & “Cloud”

- Organisations increasingly want to:
  - Reduce costs by out-sourcing commodity services to third party service providers.
  - Use their own managed identities to provide SSO and enable conformance to data protection legislation.
- SAML provides this for Web-based services...
- ...but not other types of non-Web services (IMAP, POP3, SMTP, CalDAV, etc).
- Identity Provisioning APIs exist, but they’re typically not appropriate.

Use-case 2: Web single sign-on

- Web single sign-on is widely used to manage access to content provided by third-parties.
- Contemporary Web federation technologies have some scaling limitations:
  - Identity Provider discovery
  - Managing multiple identities
  - Trust management

Use-case 3: High Performance Computing

- HPC facilities are increasingly important facilities.

- Requirements:
  - Improve Business Continuity by federating access to HPC facilities.
  - Offer HPC-as-a-service to external customers.
  - Reduce costs incurred in operating HPC-specific authentication service.
  - Provide a better user experience.

Use-case 4: Grid infrastructure

- Some users find certificates difficult to manage.
- Federate access to Grid resources
  - Authentication using certificate or non-certificate credential.
  - Authorisation using attributes (e.g. for virtual organisations).

Project goals

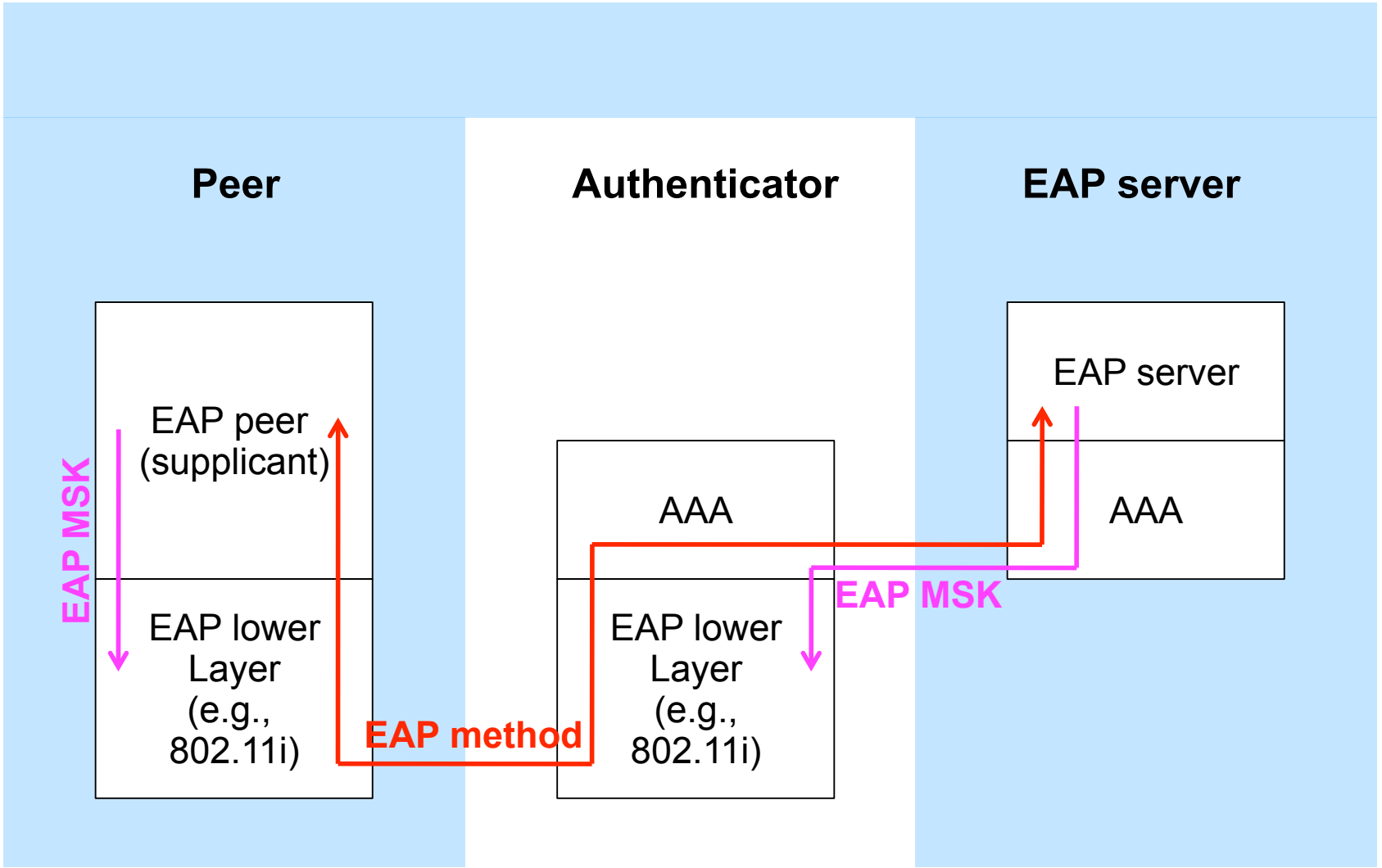
- To deliver by August 2011
  - A standardised architecture.
  - A production-quality open-source implementation.
  - Packaged and shipped with Debian Linux.
  - A test-bed for interoperability testing.
  - High quality documentation.
  - An active community of users and developers.

- To enable
  - Third-party implementations by vendors and other communities.
  - Available for all computing platforms.

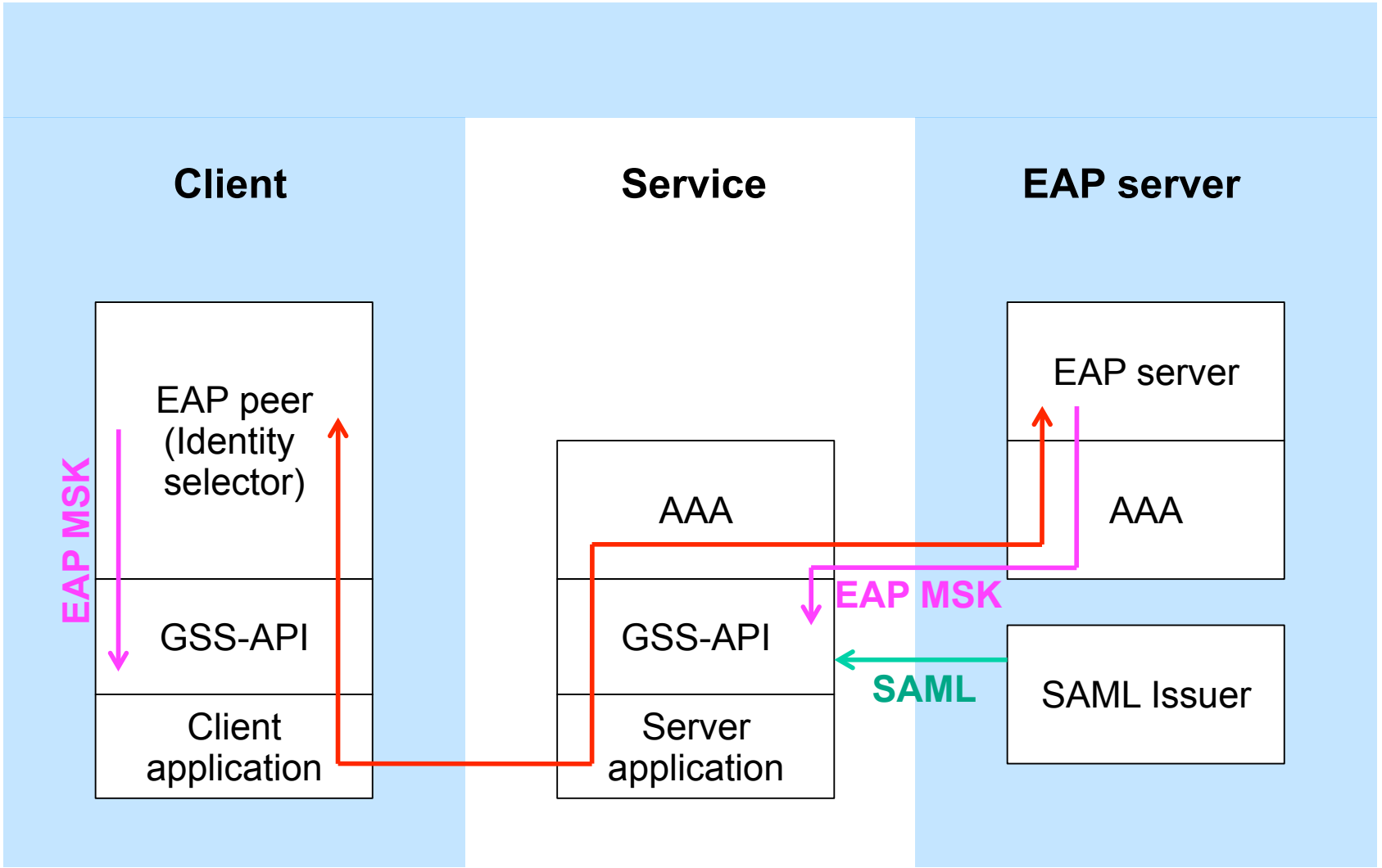
Underlying technologies

- EAP
  - provides authentication using existing mechanisms.
- SAML
  - provides authorisation using attributes.
- GSS-API
  - provides a strategy for application integration.
- RADIUS
  - Provides highly scalable federation

Background: EAP for network access



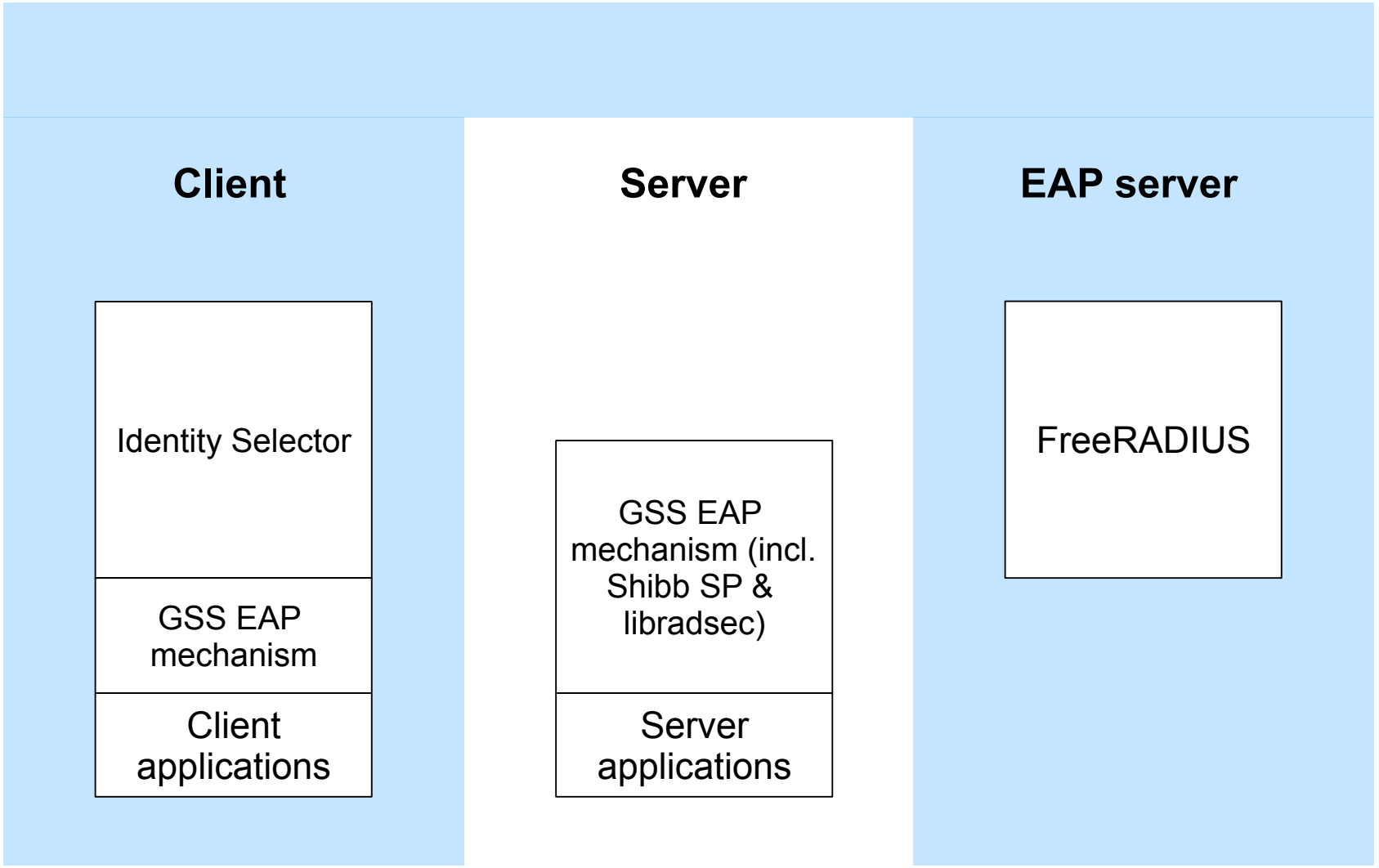
Moonshot


Client
Service
EAP server
EAP peer (Identity selector)
GSS-API
Client application
AAA
GSS-API
Server application
EAP server
AAA
SAML Issuer
EAP MSK
EAP MSK
SAML

Infrastructure software status

- GSS-API
  - Implemented a new GSS EAP mechanism for Linux and Mac OS X; Windows port planned.
- SASL
  - Supported through a new Cyrus SASL GS2 plug-in.
- Shibboleth Service Provider
  - Extended to provide important infrastructure functionality (SAML processing) for the GSS EAP mechanism.
- Libradsec
  - Provides important functionality (RadSec support) for the GSS EAP mechanism.
- FreeRADIUS
  - Will shortly be extended to support EAP channel bindings.
- Identity Selector
  - GTK-based client software that enables users to manage their identity(s), and select one for authentication when required; Windows port planned.

Infrastructure software



Application software status

- Apache
  - Implemented *mod_auth_gss* authentication module, based on *mod_auth_kerb*.
- Firefox
  - Updated Firefox's existing GSS support.
- OpenSSH
  - No modifications required to client; server requires patching.
- Adium & Jabberd
  - No modifications required to client or server.
- OpenLDAP
  - No modifications required to client or server.
- MyProxy
  - Very minor patch required.

Standardisation status

- New IETF working group using the Moonshot architecture as a starting point.
- Chaired by Klaas Wierenga (Cisco) and Leif Johannson (NORDUnet).
- Making good progress at present.
- Deliverables to be completed by Dec 2011.

Technology pilot

- Software is available for *experimental use*.
- Production-ready software will be ready in Q3 2011 with support for:
  - Linux clients and servers
  - Windows clients
- JANET(UK) is planning a Technology Pilot to explore the use of the software.
- This is likely to commence in Q3 2011.

Get involved!

- Your opinions, ideas and use-cases
  → BoF tonight, or josh.howlett@ja.net
- Join the Project Moonshot mailing list
  → moonshot-communty@jiscmail.ac.uk
- Join the IETF ABFAB mailing list
  → http://tools.ietf.org/wg/abfab
- Participate in the technology pilot
  →BoF tonight, or josh.howlett@ja.net
- Experiment with our code
  → http://www.project-moonshot.org/developers


http://www.project-moonshot.org
Project partners
JANET(UK) (http://www.ja.net)
GÉANT (http://www.geant.net)