Project Moonshot

European AFS & Kerberos Conference 2010

Pilsen, Czech Republic

13 September 2010

Josh Howlett, Middleware Architect, JANET(UK)

Background

- JANET(UK) delivers advanced networking services to the UK Research & Education community.
- Rapid deployment of trust and identity services.
- Campus, national and international levels.

Background

- Large bag of security frameworks, often bound to specific application domains:
  - Kerberos: intra-Enterprise applications
  - SAML: inter-Enterprise Web SSO
  - EAP: network authentication (802.1x, PANA, …)
  - X.509: TLS credential, Web Services, …
  - Etc.

Background

- Multiple non-interoperable security/application silos → complexity, cost & confusion.
- Moonshot is a general framework for
  - establishing trust between system entities
  - conveying identity between system entities
- In the Moonshot architecture, the first is a special case of the second.

Goals

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

- Ambitious, but achievable

  "[Project Moonshot] aims high but the potential benefits justify the effort"

  It's the F-Word, IETF Journal (June 2010)

Goals

“It might be apropos to note that the name "Moonshot" in the Moonshot proposal comes from a statement I made on a list that if you're going to change the client … and your solution is predicated on getting browser and/or OS vendors to actually move the ball, there's little point in taking halfway steps. **Design a better solution and build it**, i.e. shoot for the moon.”

Scott Cantor (IETF Kitten mailing list).

Use-case 1: Out-sourcing

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

Use-case 2: High Performance Computing

- HPC facilities are increasingly critical to Institutions.

- 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 3: Learning from Web SSO

- In federating authentication for new applications, avoid problems already discovered with Web SAML federation (and fix them).
- As a federation grows in size
  - Users are presented with an ever-growing list of identity providers (“IdP discovery problem”).
- As a federation grows in scope
  - Users may acquire more than one identity provider (“multiple affiliations problem”).

Proposed benefits

- Users
  - Users can authenticate using one or more identities to desktop applications.
  - Users can easily select an identity.

Proposed benefits

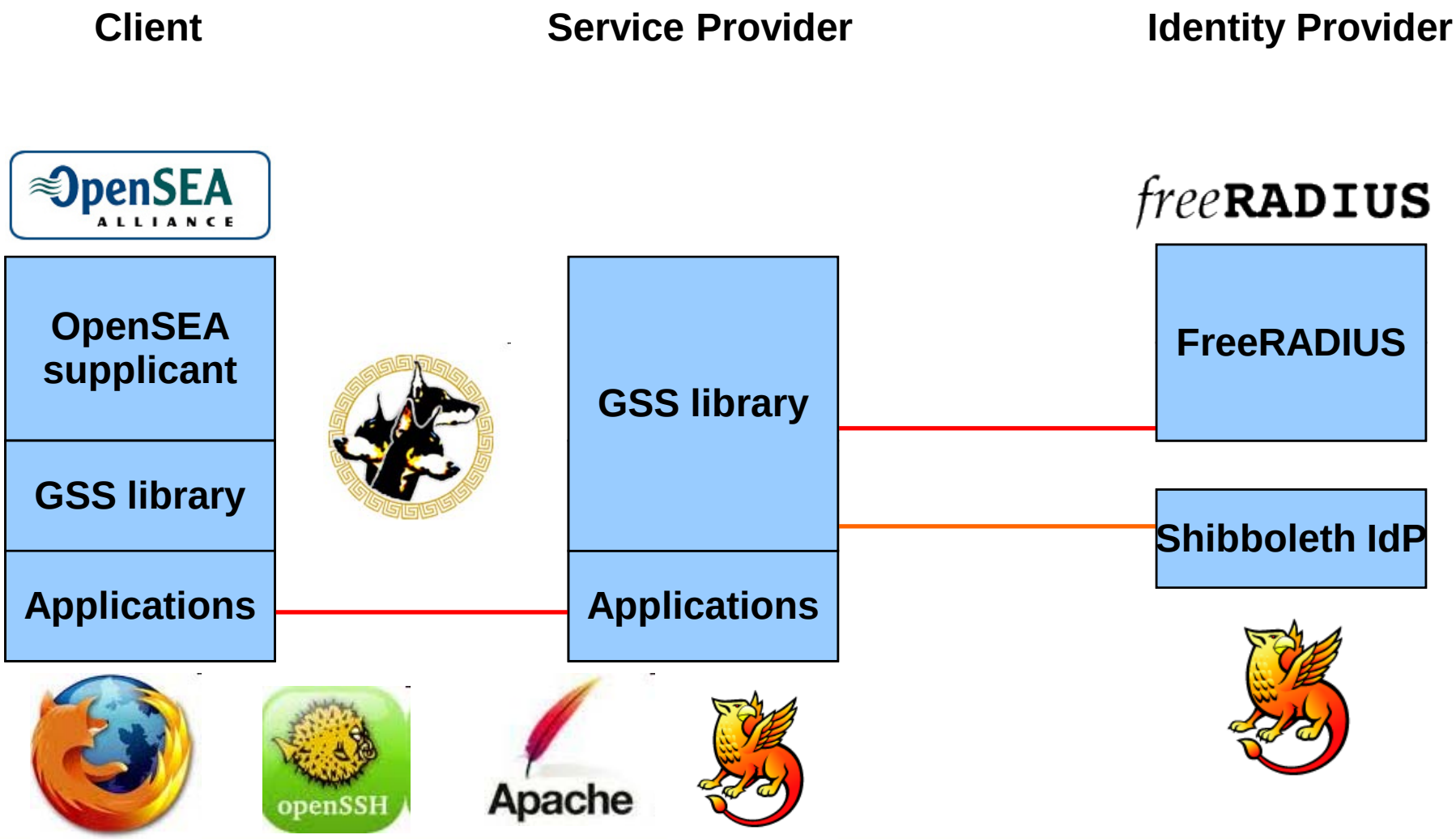
- Campuses
  - Increases the ROI made in federated identity services, by expanding its use to a greater range of applications.
  - Reduces the effort required to support different authentication technologies and credentials for different services.

Proposed benefits

- Service Providers
  - Introduces the benefits of federated identity to new types of services.
  - Addresses some of the issues associated with the conventional Web SSO.
  - The technology, when used with a web browser, could co-exist with conventional Web SSO profiles.

Moonshot architecture

By analogy with eduroam



Moonshot & Kerberos

- Moonshot and Kerberos are complementary.
- Can we leverage Kerberos?
  - Reduce impact on applications
  - Delegation
- FAST pre-authentication framework
  - Moonshot pre-authentication mechanism?

Strategy

- Work with other interested parties to reach agreement on the problems.
  - Vendors & International R&E community.
- Develop technical standards to address these.
  - IETF & OASIS.
- Develop a proof-of-concept implementation.
- Facilitate roll-out of technology for broader use.

What have we achieved so far?

- Phases 1-3 (January 2010 → April 2010)
  - Feasibility Analysis & draft specifications.
  - Bar BOF @ IETF 77.
- Phase 4 (April 2010 → June 2010)
  - Developed draft project plan.
  - Developed IETF Working Group charter.
- Phase 5 (June 2010 → August 2010)
  - IETF 78 “FedAuth” BoF: consensus to establish a working group.
  - Project plan completed
    - See http://www.project-moonshot.org/plan

Current activities

- Phase 6A (August 2010 → January 2011)
  - Advance specifications through IETF and OASIS.
  - Develop the core technology
  - Proof of concept demonstrator.

- Phase 6B (February 2011 → July 2011)
  - Develop remaining technologies.
  - Implement test-bed.

Get involved!

- Your opinions and ideas.
- Use-cases, use-cases, use-cases.
- Join the IETF AbFab mailing list.
- Join our project mailing list.
- Participate in the test-bed.

Thank you for your attention.

Any questions?

http://www.project-moonshot.org

https://www.jiscmail.ac.uk/cgi-bin/webadmin?A0=moonshot-community

josh.howlett@ja.net