Project Moonshot

MACE briefing

1 March, 2010.

Josh Howlett, JANET(UK)

Introduction

- TERENA TF-EMC2 *Beyond Web SSO* work item
- Project Moonshot use-case categories
  1. *Beyond Web SSO* - to extend the scope of federated identity to many more entities.
  2. *Scalable Trust* - to cope with “many more entities”.
- *Feasibility Analysis* by Sam Hartman
  - “technically feasible...should substantially address both of the use-cases”
- Why I'm here:
  1. to explain Project Moonshot
  2. to help move the discussion forwards: ultimately, we're happy with any solution(s) that satisfies the use-cases.

Use-cases

- Improving SAML Web Browser SSO
  - Address the “discovery” and “multiple affiliation” problems.
- Federated SSH
  - Address HPC community requirements (Business Continuity & HPC-as-a-service)
- Entity trust establishment
  - Scalable and dynamic trust establishment between SAML entities.

Expected benefits I

- Users
  - Single sign-on using one or more identities to desktop applications.
  - Selection of an identity using a client-based “identity selector”.
- Institutions
  - Use federated identity with a range of services, improving usability and reducing effort to support different authentication systems and credentials.
  - Addresses aforementioned issues with Web SSO.
  - Increases ROI already made in federated identity.

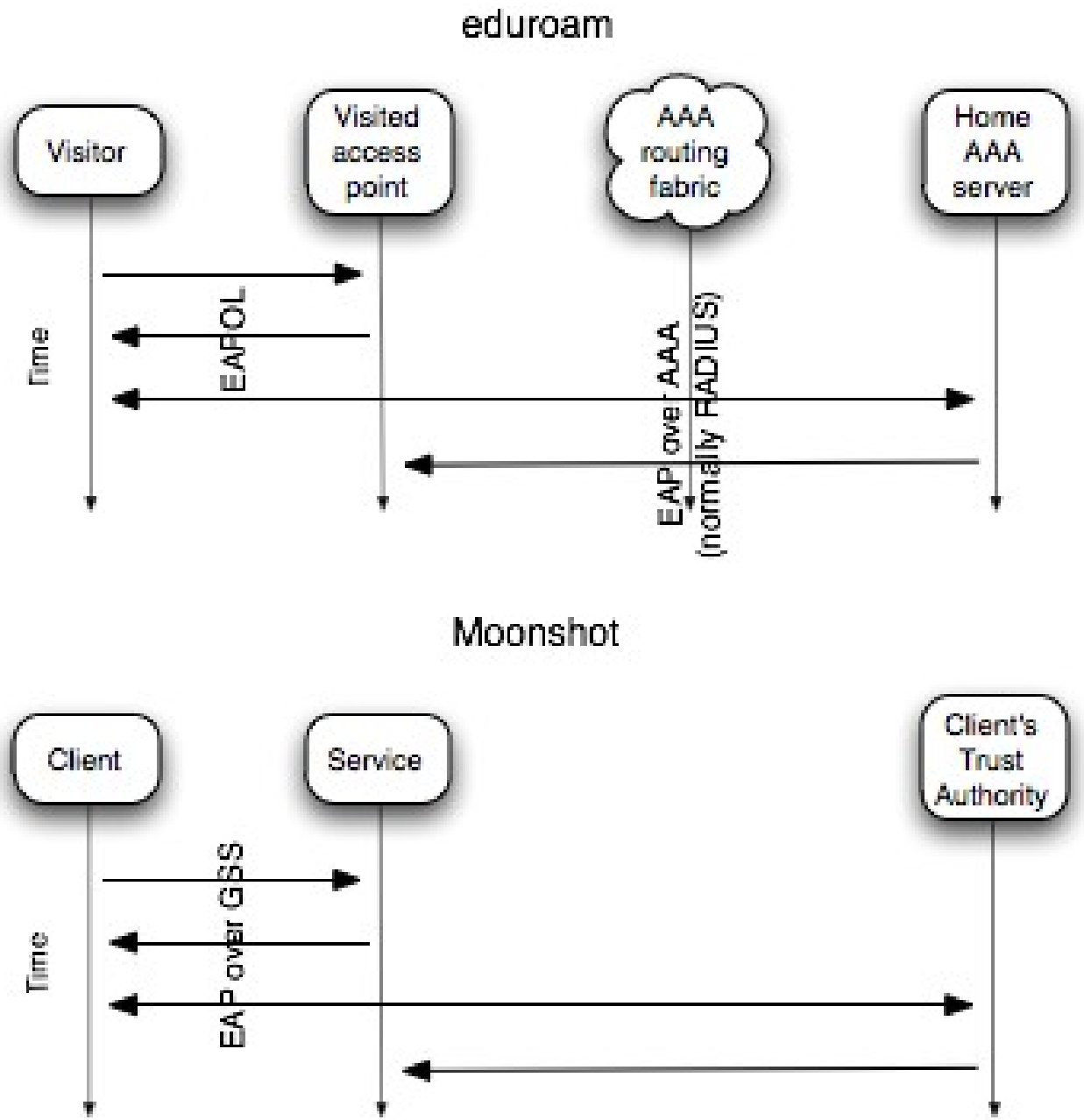
Expected benefits II

- Service providers
  - Introduces the benefits of SAML-based federated identity to new types of services.
  - Addresses aforementioned issues with Web SSO.
  - Co-existence with conventional Web SSO.
- Federation operators
  - Permits use of entity metadata without certificates, keys, key names, etc.
  - Permits use of unsigned metadata obtained from any source; the ability to establish trustworthiness of metadata; and real-time revocation.

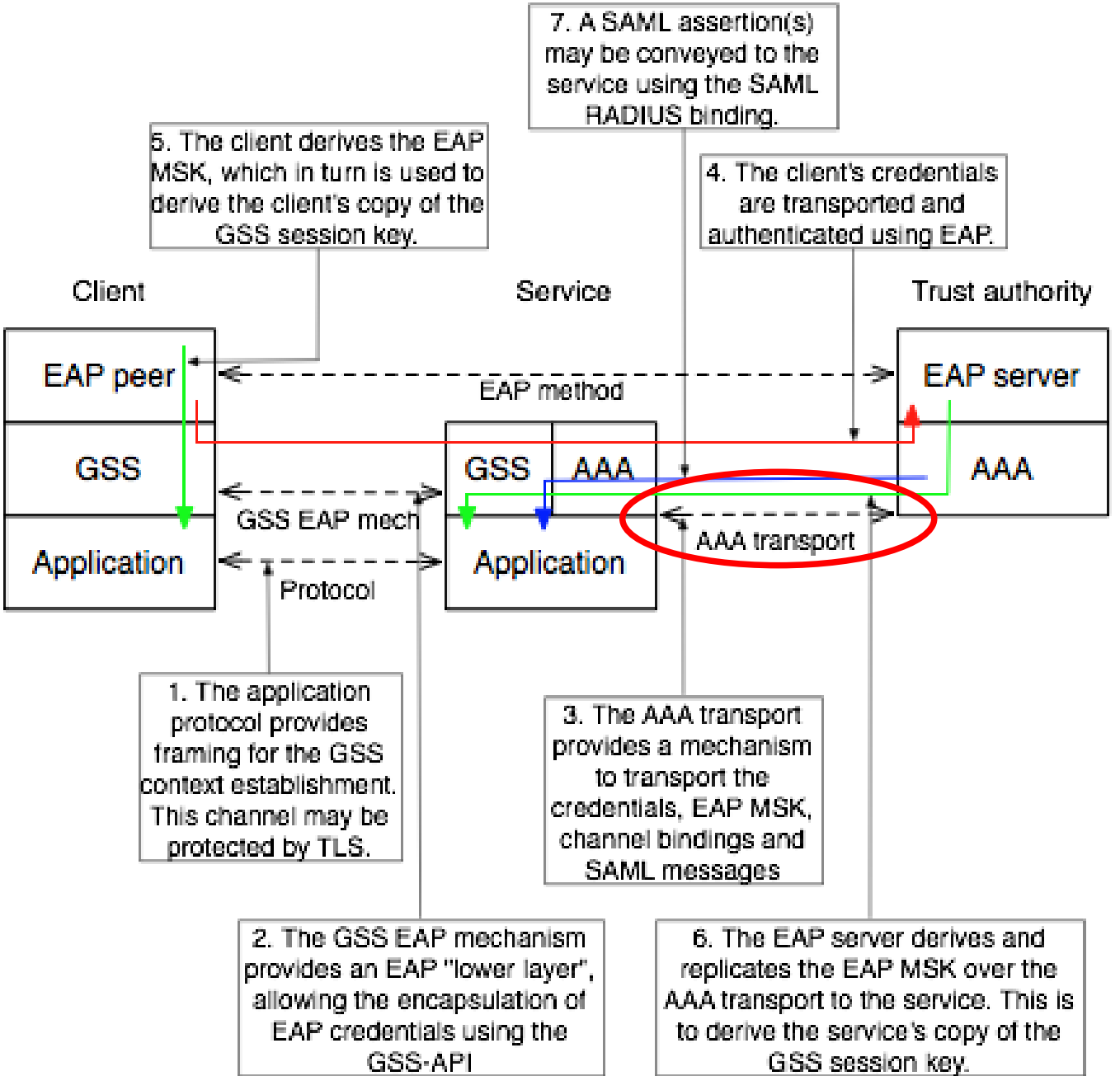
Expected benefits III

- SAML implementations
  - Provides a SAML-based SSO profile enabling federated identity for arbitrary applications without requiring significant profiling.
  - Entities can use any type of credential; interacting SAML entities do need to understand each others' credentials.
  - Credential and key management delegated entirely outside of SAML implementation.
- Standards developers
  - Provides a SAML-based SSO profile to support federated identity without significant profiling.

Analogy with eduroam



SAML EAP Profile



3-5 year vision

- Clients have a common user & system interface for obtaining access to applications and networks.
- All services can use a common technical approach for controlling access.
- Trust authorities use a common technical approach for authentication of users and entities, using credentials of their choice.
- Dynamic and scalable trust establishment between trust authorities.

Moonshot planning

- January 2010 → April 2010
  - Technical feasibility analysis
  - Business analysis & strategy development
- April 2010 → July 2010
  - Development of draft specifications
  - Locate partners (GN3, NRENs, others)
  - Establish IETF Working Group
- August 2010 → July 2011
  - Advance specifications within SDOs (IETF/OASIS)
  - Software development
  - Implement test-bed demonstrating the use-cases

Proposed outline of work

- Specifications
  - EAP GSS mechanism (IETF)
  - RADIUS SAML attributes (IETF)
  - EAP channel bindings (IETF)
  - SAML RADIUS binding (OASIS)
  - SAML EAP Profile (OASIS)

Proposed outline of work

- Software development
  - GSS library: consultant, non-GN3 funded
  - FreeRADIUS: consultant, non-GN3 funded
  - Open1x: consultant or GN3, {non-}GN3 funded?
  - mod-auth-kerb: GN3
  - Firefox: GN3
  - Shibboleth SP: some modifications required
  - Shibboleth IdP: no modifications required?
  - SSH client and server: GN3?

Outline of work

- Proof of concept test-bed
  - Enhanced Web SSO: GN3?
  - Federated SSH: GN3?
  - Entity trust establishment: GN3?

Conclusions

- Addresses SSO for non-web applications and trust establishment using a common technical approach.
- Technically feasible; more work required to determine business acceptability.
- Touches a lot of existing technology, but changes required are generally modest.
- New partners are welcome!
- There's a mailing list:

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