Project Moonshot

TF-EMC2 & TF-Mobility

Vienna, 17th February

Josh Howlett, JANET(UK)
Introduction

"[I]f you go for a complete client stack revamp [...] then I would shoot for the moon."

Scott Cantor, REFEDS mailing list, 22 October 2009.
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”.
- Independent *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

“To infinity, and beyond!”

Buzz Lightyear
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 can't believe that!" said Alice.

"Can't you?" the queen said in a pitying tone. "Try again, draw a long breath, and shut your eyes."

Alice laughed. "There's no use trying," she said. "One can't believe impossible things."

"I dare say you haven't had much practice," said the queen. "When I was your age, I always did it for half an hour a day. Why, sometimes I've believed as many as six impossible things before breakfast."

'Alice in Wonderland', Lewis Carroll
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.
Proposed architecture

“We shape our buildings; thereafter they shape us.”

Winston Churchill
Analogy with eduroam
SAML EAP Profile

1. The application protocol provides framing for the GSS context establishment. This channel may be protected by TLS.

2. The GSS EAP mechanism provides an EAP "lower layer", allowing the encapsulation of EAP credentials using the GSS-API.

3. The AAA transport provides a mechanism to transport the credentials, EAP MSK, channel bindings and SAML messages.

4. The client's credentials are transported and authenticated using EAP.

5. The client derives the EAP MSK, which in turn is used to derive the client's copy of the GSS session key.

6. The EAP server derives and replicates the EAP MSK over the AAA transport to the service. This is to derive the service's copy of the GSS session key.

7. A SAML assertion(s) may be conveyed to the service using the SAML RADIUS binding.
Scalable Trust

“In general, SAML itself defines nothing related to trust management […] In fact, absolutely nothing in the standards world addresses this. Makes writing this stuff fun.”

https://spaces.internet2.edu/display/SHIB/TrustManagement
Step 1: simple AAA trust
Step 2: basic federation
Step 3: Introducing the trusted third party
An interlude: the Moonshot Key Negotiation Protocol

- A general mechanism for establishing a security context between two network entities.

- The Key Negotiation Profile is the SAML EAP Profile bound to HTTP.

- It provides a REST-based web-service that clients can invoke to establish a security context using their EAP credential.
Step 4: Using the MKNP to establish dynamic AAA relationships
Step 5: Recursive discovery
Entity trust establishment

Some surprising properties:

1. Metadata consumer and target entity establish keys dynamically.

2. Metadata can be obtained via any mechanism, trusted or not.

3. The entities do not need to share a common credential technology.

4. Provides a scaleable solution to inter-federation.
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

• Now → July 2010
  • Development of draft specifications
  • Locate partners (GN3, NRENs, others)
  • Establish IETF Moonshot Working Group

• August 2010 → July 2011
  • Advance specifications within SDOs (IETF/OASIS)
  • Establish IETF working group
  • Develop software components
  • Implement a test-bed demonstrating the use-cases
Proposed outline of work

• Specifications
  • EAP GSS mechanism (IETF): rough draft
  • RADIUS SAML attributes (IETF): rough outline
  • EAP channel bindings (IETF): conceptual
  • SAML RADIUS binding (OASIS): solid draft
  • SAML EAP Profile (OASIS): conceptual
  • Key Negotiation Profile (OASIS): conceptual
  • 'Moonshot Trust Profile' (OASIS): rough outline
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: ?
  - Shibboleth IdP: consultant or GN3, {non-}GN3 funded
  - SSH client and server: GN3
Outline of work

- Proof of concept test-bed
  - Enhanced Web SSO: GN3
  - Federated SSH: GN3
  - Metadata: GN3
Conclusions

• Addresses several problems previously considered hard or intractable using a *single technical approach*.

• Provides several other interesting benefits.

• Standards work has begun; initial drafts hitting IETF and OASIS shortly.

• Who want to help build it...?