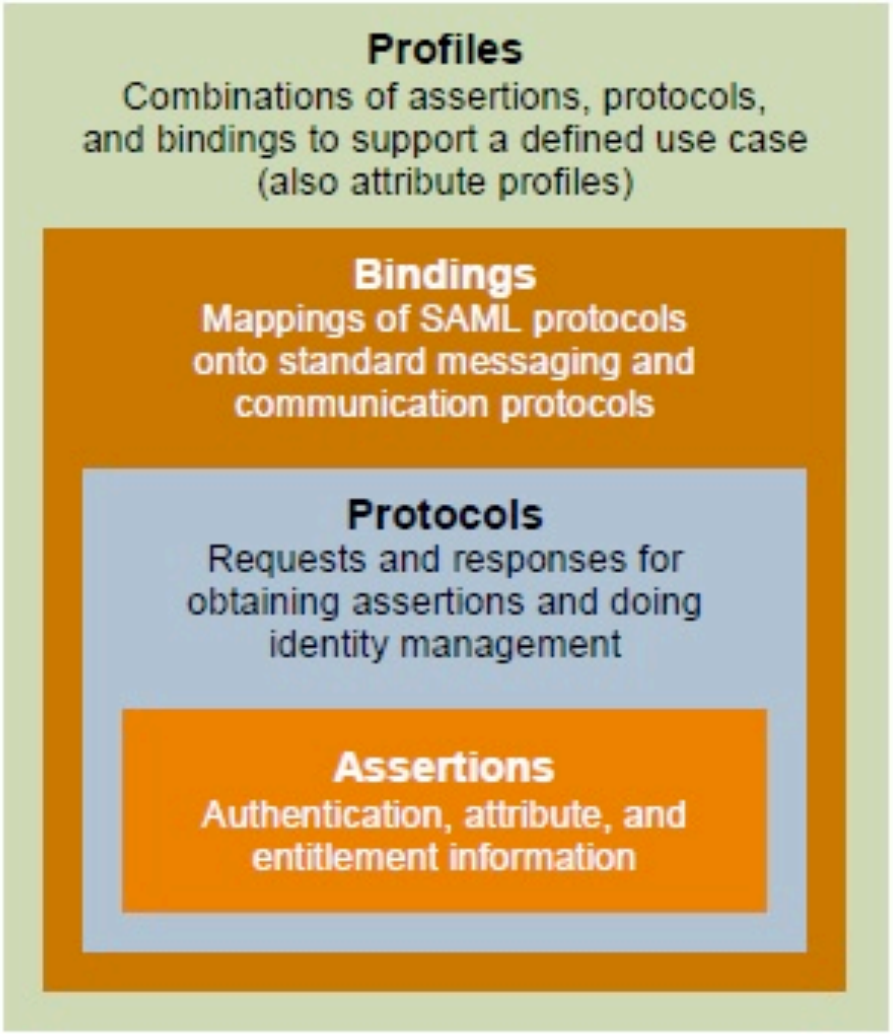
draft-ietf-abfab-aaa-saml

Josh Howlett, JANET

IETF 82

SAML components and how they relate to each other

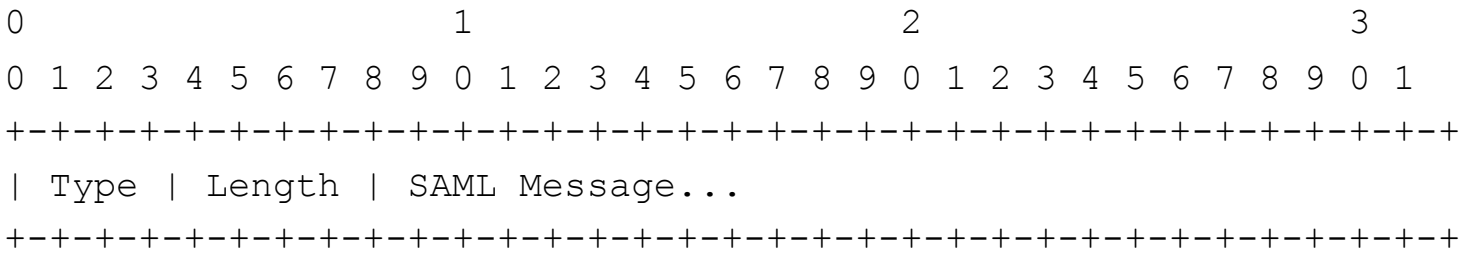


Abfab Authentication Profile &
Abfab Assertion Request Profile

SAML RADIUS binding &
SAML RADIUS attribute

In SAML, bindings typically use HTTP or SOAP transport. ABFAB is defining a RADIUS binding.

SAML RADIUS Attribute

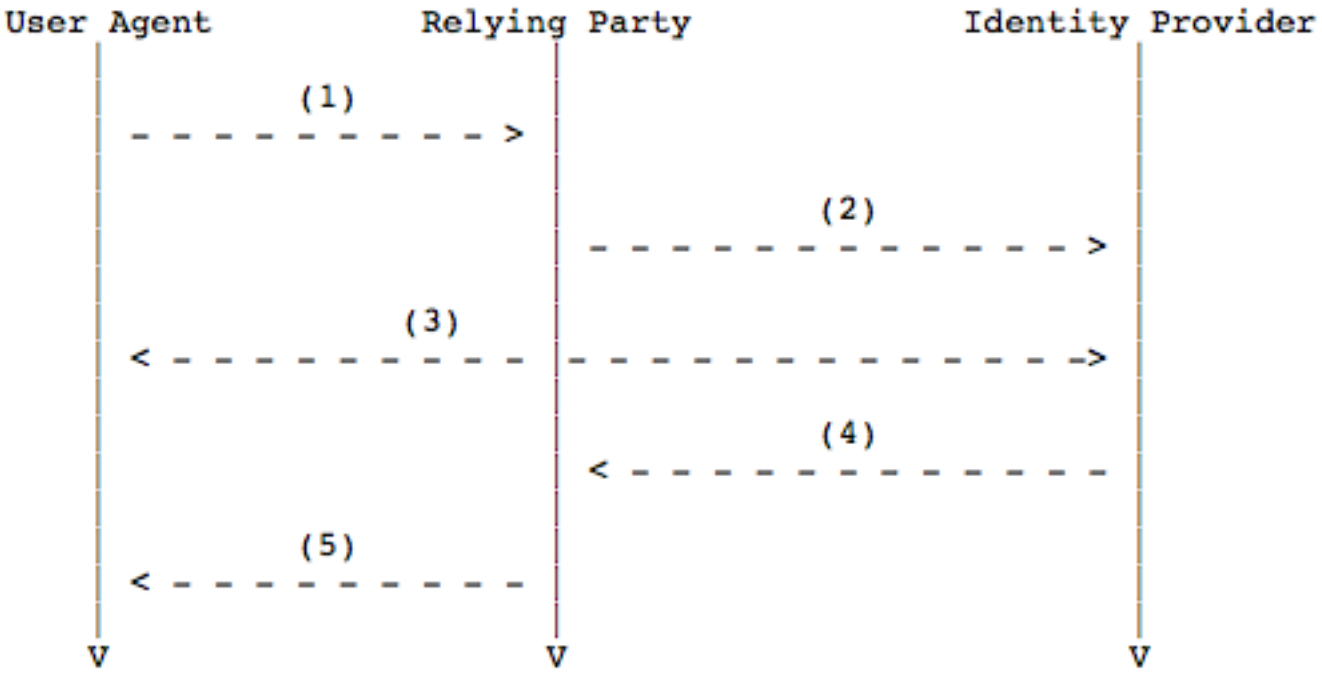


SAML RADIUS Binding

- SAML requester is RADIUS client / RP
- SAML responder is RADIUS server / IdP
- SAML protocol message is encapsulated within (and fragmented across multiple instances of) the SAML RADIUS attribute
- NAI is used to route RADIUS messages from the SAML requester towards the SAML responder
- Attribute is currently defined independently of the Binding, to facilitate use in other contexts – is that actually useful, or a complication?

Abfab Authentication Profile

- A profile of the SAML Authentication Request Protocol that uses the SAML RADIUS binding



Abfab Assertion Request Profile

- TODO
- Intend to specify a profile of SAML “Assertion Query and Request Protocol” using the SAML RADIUS binding
- Requirements
  - Request assertion from authentication IdP, after authentication
  - Request assertions from other attribute sources

Issue: document name

- Name includes “aaa”, but only discusses RADIUS
- Currently named “A RADIUS Attribute, Binding and Profiles for SAML”
- Sufficient?

Issue: signatures

- Use of SAML signatures
  - Profile (but not binding) currently prohibits use of SAML signatures
    - Encourage use of transport integrity protection, reducing deployment complexity
    - Reduce size of SAML messages
  - Limited support
  - Proposal: require NASes to default NOT to check signatures; and indicate that signatures are not required

Issue: SAML payload size

- RADIUS message MTU of 4kb, but SAML messages can be arbitrarily large
  - Option 1: Do nothing
  - Option 2: If >4kb, advise deployments to use Diameter
  - Option 3: Use a SAML SOAP-based transaction to request attributes or resolve an artifact
  - Option 4: Develop a RADIUS-based mechanism to fragment large payloads over multiple RADIUS messages

Todo

- Fix various nits
- Define attribute request profile