

An AAA Attribute for SAML Constructs

draft-ietf-abfab-aaa-saml-00

Josh Howlett, JANET(UK)

ABFAB @ IETF79

Problem statement

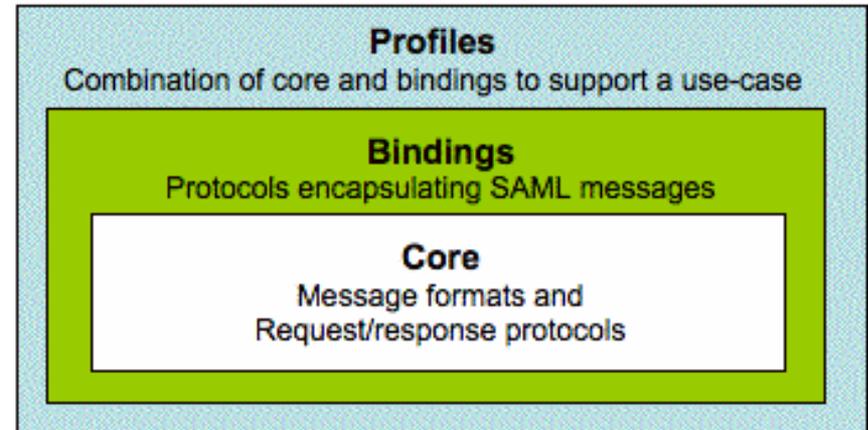
- Permit use of SAML authentication and authorisation semantics.
 - Avoid re-invention of semantic wheels (e.g., attribute profiles, authentication context, subject confirmation).
- SAML already defines several HTTP transports, but these call-backs may:
 - Be chatty.
 - Complicate the trust model.
 - Increase AAA client implementation complexity.
- Can we transport SAML in-band?

Design considerations

- A SAML construct can be arbitrarily large, but:
 - Maximum RADIUS attribute length is 254 bytes.
 - Maximum RADIUS message size is 4096 bytes.
 - Even **if** that were increased, UDP transport is limited to 64kb.
- None of this is good, but not necessarily fatal depending on the use-case in question.
- Diameter resolves this.
 - Should ABFAB RECOMMEND the use of Diameter?
- draft-ietf-radext-tcp-transport would assist the use of RADIUS if the (arbitrary) message size were increased.

Design considerations

- SAML defines a three layer conceptual model:
 - message syntax and PDUs ('core')
 - transport ('bindings')
 - profiles (a slice through 'core' + 'bindings').
- AAA attribute + AAA protocol = Binding.
- SAML bindings *almost* always only transport Request/Response messages, but sometimes also 'naked' assertions.
- But some other SAML constructs might also conceivably be useful (e.g., artefacts).

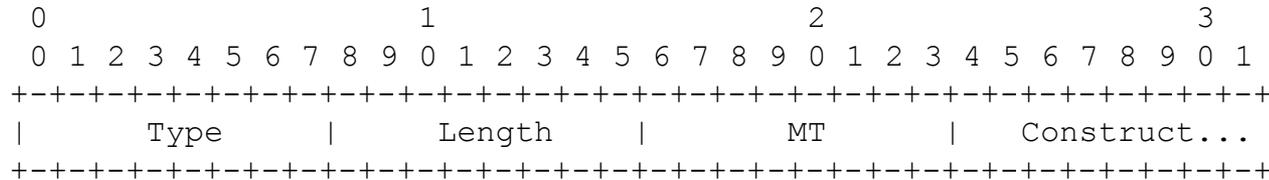


- We can probably satisfy the ABFAB requirements with a naked assertion; but should we shoot for something more general?
 - e.g. If we want to allow the AAA client to stipulate specific attributes in the Response assertion.
 - There may be other use-cases of this attribute other than ABFAB, e.g. network access authorisation.

Design approach

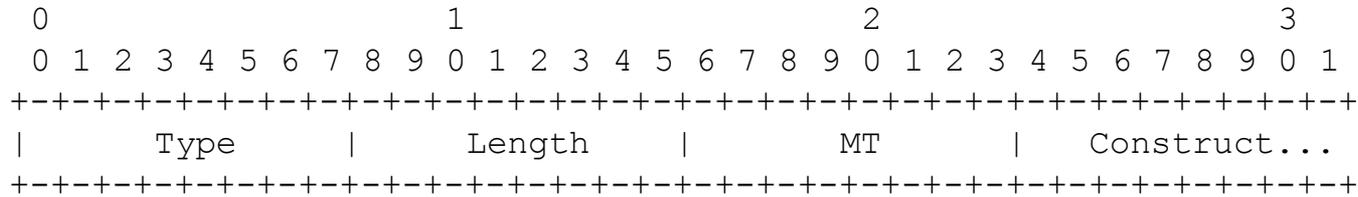
- RADIUS formatted attribute
 - Define Diameter AVP for Diameter transport?
- Simple internal format that is intended to support a range of SAML constructs
 - Using an 8 bit namespace...
 - Currently only SAML Request/Response elements are named.

Current design



- Construct Type (CT)
 - “The Construct Type field is a one octet enumerated field. It takes an integer value denoting the type of SAML construct in the Construct field.
 - TBD SAML Request protocol element
 - TBD SAML Response protocol elementAll other values are reserved for IANA allocation subject to the provisions of section 5.”
 - Intended to indicate the type of construct to a AAA client/server, without needing to parse it directly. But is this important?

Current design



- Construct
 - “The Construct field is one or more octets containing a SAML construct. If larger than a single attribute, the SAML construct data **MUST** be split on 253- octet boundaries over as many attributes as necessary. On reception, the SAML construct is reconstructed by concatenating the contents of all SAML-Construct attributes.”

Input required

- Should ABFAB RECOMMEND the use of Diameter?
- Define Diameter AVP for Diameter transport?
- We can probably satisfy the ABFAB requirements with a naked assertion; but should we try to shoot for something more general?
- The CT field indicates the type of construct to a AAA client/server, without needing to parse it directly. But is this important?