draft-ietf-abfab-aaa-saml

ABFAB

IETF 86
Network Access Identifier Name Identifier Format

• A SAML ‘name identifier format’ defines syntax and semantics for different types of names (Kerberos, email, X.509, etc).

• This document now defines an NAI name identifier format

• This enables Subjects of SAML assertions and requests/queries to be named by NAI
RADIUS State Confirmation Methods

• Defines two new ‘Confirmation Methods’ for SAML, for ‘users’ and ‘machines’ respectively
• “[I]ndicate[s] that the Subject is the system entity (either the user or machine) authenticated by a previously transmitted RADIUS Access-Accept message, as identified by the value of that RADIUS message's State attribute.”
• The purpose is to enable the RP to identify a Subject by RADIUS State value, rather than by a SAML Subject value; this simplifies implementation of some use cases.
• Question: should we explicitly link these to the ‘user’ and ‘machine’ TLV definitions proposed by TEAP?
SUBSTANTIVE CHANGES
RADIUS SAML binding

- This binding defines how SAML messages are transported by RADIUS

- Support for RADIUS UDP changed from MUST to MAY

- Support for RADIUS TLS changed from RECOMMENDED to REQUIRED

- Support for perez-radext-radius-fragmentation changed from MUST to MAY
ABFAB URN registry

• A new top-level registry is created titled "ABFAB Parameters"
  – urn:ietf:params:abfab:foo:bar

• This is used to name the following SAML constructs:
  – bindings:radius
  – nameid-format:nai
  – profiles:authentication
  – profiles:query
  – cm:user
  – cm:machine
OTHER CHANGES

draft-ietf-abfab-aaa-saml
Other changes

• Expunged some repetitive text in the ‘Introduction’ section
• Now talks exclusively about ‘EAP’, rather than ‘GSS EAP’
  – Accordingly GSS terms such as initiator and acceptor have been replaced with the appropriate EAP equivalents
TODO

• Figure out a way to name SAML authorities (e.g., attribute authorities) to support synchronous requests (e.g., for assertions).
• The document currently only discusses TLS/TCP; also should mention TLS/UDP
• Include a prescription that “SAML responders SHOULD return a RADIUS state attribute” to facilitate subsequent use of the user/machine Subject Confirmation methods
• Clarify text describing use of the SAML AuthNRequest’s ‘AllowCreate’ attribute