draft-ietf-abfab-aaa-saml

Sam Hartman

ABFAB

IETF 88, Vancouver

Status update

- The Good News
  - All out-standing discussed at IETF 87 believed addressed
  - All requested functionality believed incorporated
- The Bad News
  - Some use of terminology is inconsistent with the Architecture document: alignment required
  - Some of the text is fairly terse in places, and may require elaboration to improve comprehension.
  - Text needed for Security & Privacy Considerations sections

Open Issue: ForceAuthn

"If the ForceAuthn attribute on the <samlp:AuthnRequest> element (if sent by the requester) is present and true, the Identity Provider MUST freshly establish this identity rather than relying on any existing session state it may have with the Principal (for example, TLS state that may be used for session resumption)"

- Requires interactions between SAML and EAP state machine. Is MUST appropriate?

Open Issue: Naming

- Section 5.3.2 (SAML names) talks about SAML responses checked against realms specified in the response or in metadata.
- No way to do that.
- Do we care?

Open Issue: Which RADIUS message

- 7.3.2 – “The Relying Party MAY include a <samlp:AuthnRequest> within this RADIUS Access-Request message“
- Which message?
  - First? All?

Next steps

- Would appreciate help on
  - Expert review on the document's definition of the two extended RADIUS attributes
  - "Non-expert review" to identify areas of text requiring elaboration, examples, etc.
  - Contributions (even if just identifying issues requiring discussion) to the Security & Privacy sections.

- Aiming for WGLC by next IETF