draft-ietf-sip-saml-02.txt

thanks to reviewers

- Erkki.Koivusalo
- Shida Schubert
- Jiri Kuthan
- steffen.fries
- Marcos Dytz
- Keith Drage
- Andreas Pashalidis
- Richard Barnes
- marc.willekens
- Mayutan Arumaithurai
- Sebastian Felis

Nature of Feedback

- overall: Yes, worthwhile to do this spec
- technically specific feedback
  - categorized as:
    - Substantive
    - Security Considerations
    - Desired Clarifications
    - Editorial

Substantive Feedback

- RFC4474 Identity-Info header field referent issue
- Authorization assertion delivered only by reference – no by-value delivery, contravening RFC4484
    - i.e. address additional use cases?
- Use “redirection” rather than “proxy mode”

RFC4474 Identity-Info header field referent issue

- key adjacent sentences in RFC4474 (section 9, page 15):
  - The 'absoluteURI' portion of the Identity-Info header MUST contain a URI which dereferences to a resource containing the certificate of the authentication service.
  - All implementations of this specification MUST support the use of HTTP and HTTPS URIs in the Identity-Info header.
  - Such HTTP and HTTPS URIs MUST follow the conventions of RFC 2585 [10], and for those URIs the indicated resource MUST be of the form 'application/pkix-cert' described in that specification.

RFC4474 Identity-Info header field referent issue (cont'd)

- Peterson & Jennings recommend:
  - stating in -sip-saml-03 that..
    - The URI references defined by this spec (sip-saml) are not the ones referred to by the 3d sentence of the RFC4474 stipulation of Identity-info header field contents.
  - ..and possibly also..
    - investigate “tagging” the http(s): URIs referencing assertions via something akin to RFC2585's approach
- Thoughts?

no by-value delivery, contravening RFC4484

- RFC4484 “Trait-Based Authorization Requirements for SIP”
  - Section 5, page 11: “Trait-Based Authorization Requirements”
  - includes statement:
    - Authorization services MUST be capable of delivering an assertion to a SIP UAC, either by reference <u>or by value</u>.
- Are there additional use-cases that we *need* to address at this stage?
  - If not, then it's ok to not strictly adhere to RFC4484

Use “redirection” rather than “proxy mode”

- The comment is:
  - use redirection as opposed to proxy mode. IMO, it is beneficial to have the AS operated in 3xx mode for better scalability.
- From RFC3665 section "3.6. Session via Redirect and Proxy Servers with SDP in ACK":
  - it isn't clear to me that there is necessarily a salient difference between it's scenario and the one depicted in draft-ietf-sip-saml-02 fig 1.

WRT remaining classes of comments

- Received these other classes of comments:
  - Security Considerations
  - Desired Clarifications
  - Editorial
- Replied on sip@ list to first two, inserted editorial comments into the “tracker”.