REFEDS assurance vc 2016-10-31

REFEDS assurance wg call 31st October 2016
13:30-14:20 (UTC), 14:30-15:20 (CET), 8:30-9:20 (CDT) -- Daylight saving over in Europe

Adobe Connect, https://connect.sunet.se/edugain

Pál
Tom
Christos
Nicolas
Mikael

Notes
- document: https://docs.google.com/document/d/15v65wJvRwTSQKViep_gGuEvxLi3UJbaOX5o9eLtsyBI/edit

Key updates since last vc:
- added a placeholder to REFEDS MFA (waiting for its approval process)
- added “The attribute quality and freshness is limited to the following values of eduPersonAffiliation and eduPersonScopedAffiliation attributes: faculty, student and member”

Items discussed:
- “The person and the credential they are assigned is traceable i.e. the Home organisation knows who they are and can contact them” (to synchronize with SIRTFI text which says “Users can be contacted. ”)
- Borderline between Identity concept (section 1) and ID proofing (section 2): Which of the two does the previous requirement belong to? Leave in identity concept.
- Entity Attributes (pertaining to all identities) or assertions (pertaining to one identity)?
  • identity concept -> assertion
  • ID proofing and credential delivery/renewal/reissuance -> assertion
  • authentication -> assertion
  • attribute quality/freshness -> assertion
  • management and organizational considerations -> Entity Attributes
- how to present the assurance statements in an assertion?
  • challenge: vector processing. How to provide RPs the processing instructions to decide if the IdP assertion is good enough
  • approach: provide (1) full vector for those RPs interested and (2) packed values where values are collapsed into single scalar values for simplicity
  • Mikael to make first draft
- how to bind the assurance statement(s) to federation protocols
  • in SAML: use authentication context
  • in OIDC:
    • ACR is single-valued (needed to overload the single-valued claim, e.g. comma-separated list of values)
    • AMR (OPTIONAL). “Authentication Methods References. JSON array of strings that are identifiers for authentication methods used in the authentication. For instance, values might indicate that both password and OTP authentication methods were used. The definition of particular values to be used in the amr Claim is beyond the scope of this specification. Parties using this claim will need to agree upon the meanings of the values used, which may be context-specific. The amr value is an array of case sensitive strings.”
  • how to present the assurance statements for Entity attributes
    • try to have just one Entity attribute to indicate that the IdP supports the REFEDS assurance profile
    • follow the SIRTFI approach and use Name="urn:oasis:names:tc:SAML:attribute:assurance-certification"

Next vc:
14 November (Daylight saving over in the US): 14:30-15:30 (UTC), 15:30-16:30 (CET), 8:30-9:30 (CST)