ATARC Identity Management Working Group Comment for NIST SP 800-217

Overall, the ATARC Identity Management Working Group did not find anything within the draft release of NIST SP 800-217 that we wished to comment on directly. With that said, the working group wishes for NIST to consider expanding this current draft, or suggest NIST to create a follow-up special publication for the purpose of creating technical guidelines for federation implementation.

The current draft of NIST SP 800-217 does not currently contain any naming schemas for those attributes required to be included within an OIDC or SAML federation. This could be detrimental to interoperability within and between agencies.

Within an agency, application developers currently do not have a standard to develop against. This has led to different interpretations of standard attributes. For example, some applications accept userprincipalname for the subject identifier, while others want samaccountname or email. This requires IDPs to be flexible in their attribute schema. This also has slowed the adoption of federation, as each application must be examined to understand which attributes can be accepted, and in which format those attributes need to be presented. As the government looks to adopt a federated identifier, as identified within NIST SP 800-217, application owners, especially those that service multiple agencies and departments, are likely to continue to implement different naming structures without a common standard.

Between agencies, the lack of a formal standard for attributes, especially with the beforementioned federated identifier, will require each agency to examine the attribute naming structure of the other agency, and modify their federation agreement(s) accordingly. This attribute mapping will be required for each agency, and, potentially, for each shared application between agencies.

What is needed is a more formal set of guidelines for attribute naming. This should be similar to how NIST defined the PIV Applet standard within the NIST SP 800-73 series. The release of NIST SP 800-73 gave application owners and industry vendors a defined structure to develop against and has resulted in a more interoperable smart card solution than would likely have occurred without this direct guidance from NIST. While it would not be practical for NIST to define the naming structure of every possible attribute, the common attributes for use by the federal government ought to be defined.