The Chairs and Members of the
OASIS Security Services (SAML) TC

November 4, 2008

William E. Burr, *et al*
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

email: eauth-comments@nist.gov

Re: Suggested revisions to Draft NIST Special Publication 800-63-1 and the use of Assertions at Level-of-Assurance 4.

Dear Colleagues:

It has recently come to our attention that the February 2008 draft revision of NIST Special Publication 800-63-1 "Electronic Authentication Guideline"**[1]** explicitly prohibits the use of "assertions" at level-of-assurance 4 (LOA-4).

While we agree that “assertion” usage described in existing published specifications (including SAML 2.0 and subsequent profiles) do not meet the strict requirements defined for LOA-4, we also feel that mechanisms exist that can be employed to provide adequate protection for assertions that will satisfy LOA-4 needs. In the particular case of SAML assertions, a draft "Holder-of-Key Web Browser SSO Profile"**[2]** now being discussed in the SSTC defines a method for achieving the required protections for using SAML Single-Sign-On (SSO) at LOA-4.

As a consequence, we are suggesting some changes to the language in the 800-63-1 draft to stipulate the conditions necessary for assertions to be used at LOA-4.

We feel that this is an important modification for several reasons

- It enhances security and economy if the same protocol suite can be deployed for use at all LOAs. Problems with configuration, maintenance, and procurement can arise when there is one set of protocols, implementations, and vendors at LOA 1-3 and a separate set of protocols, implementations, and vendors for LOA 4.
- Many organizations around the world use the NIST 800-63 publication as a model for their own authentication schemes. NIST should propose the best and most precise set of requirements while allowing for evolution in the protocols

The following are some specific changes we would suggest.

1 Justification for prohibiting assertions

The following text is found on p. 8:

> Assertions are not allowed at Level 4 since it is not possible to establish a strong enough binding between the authentication activity established between the Claimant and the Verifier, and he secure session established between the Subscriber and the Relying Party.

We would suggest the following alternative

> Assertions are only allowed at Level 4 if conveyed via protocol mechanisms that allow a strong binding between the authentication activity established between the Claimant and the Verifier, the secure session established between the Subscriber and the Relying Party, and the assertion itself.

2 Assertion Protection

Section 10.3 specifies the Assertion protections at each LOA. Currently, section 10.3.2.4 (p. 85) simply says

> At Level 4, assertions shall not be used.

We would suggest that this be modified to the following:

> Assertions are allowed at Level 4 if carried via protocol mechanisms that allow a strong cryptographic binding between the assertion and the transport mechanism used to convey the assertion between the claimant, the verifier, and the relying party.

3 Table 14

We also suggest a replacement for the last column of table 14 (p.84) which describes "threat resistance per assurance level" for assertions. We should be able, based on the text we provide for 10.3.2.4 (above), to have YES in every cell.

We also suggest the addition of a row to that table for (e.g.) "Cryptographic binding of assertion to channel" that is Yes for the Level 4 column.

Ultimately, we believe that the SAML HoK SSO profile will satisfy these requirements; updates to other protocols may also make it possible to use their versions of assertions at LOA-4 as well. Future versions of the NIST 800-63 document may make specific reference to these updated protocol profiles as they are approved in the relevant standards bodies.

Please feel free to contact us with questions about these suggestions or if further clarification is needed.

Respectfully submitted on behalf of the members of the OASIS SAML TC,

Hal Lockhart,
Co-Chair, OASIS SAML TC
hal.lockhart@oracle.com

Brian Campbell,
Co-Chair, OASIS SAML TC
bcampbell@pingidentity.com

[1] See http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-63--1

[2] N. Klingenstein. *SAML V2.0 Holder-of-Key Web Browser SSO Profile, Working Draft 07*. OASIS SSTC, 22 September 2008. See http://wiki.oasis-open.org/security/SamlHoKWebSSOProfile