Subject: [InC] Your feedback requested: consultation open for revised SAML2int
From: "Wessel, Keith" <kwessel@illinois.edu>
Date: 4/9/18, 9:04 PM
To: "participants@incommon.org" <participants@incommon.org>

Colleagues,

This message is being sent to the InCommon participants and REFEDS mailing lists. Apologies to those receiving it twice.

The InCommon Deployment Profile working group invites you to review and comment on a revised version of the SAML 2.0 Interoperability Deployment Profile. The working group has been hard at work on this revision for the past 18 months. We've covered some difficult ground and come up with a thorough and useful profile that will benefit federated service deployment internationally.

Now, we're at the point where we need your help. We're asking you to review our updated version of SAML2int and provide your feedback. Following InCommon's process for community consultation, we're opening a consultation period beginning today, April 9, and ending May 7. Links to the updated profile and the feedback page can be found here:

https://spaces.internet2.edu/x/WIPmBQ

While updating SAML2int, the working group chose to tackle some of the bigger issues that challenge federations today. To help the reader understand some of the group's decisions, here is a summary of a few of the issues and our rationale behind the requirements for these issues. This summary is also included, for convenience, at the top of the feedback page on the wiki. Feedback on the requirements for these items, as well as on anything else in the document, is of course encouraged.

Identifiers and NameIDs
This section eliminates the use of any NameID format other than transient. In addition, the complex, confusing, and in some cases poorly adopted set of attribute identifiers used today has been replaced with two clear identifiers for communicating the subject. This model leverages the new OASIS identifiers profile: https://www.oasis-open.org/committees/download.php/62438/saml-subject-id-attr-v1.0-wd04.pdf. While the identifiers profile is still in process, it continues to move toward adoption. We believe this will make the adoption of identifiers much clearer and easier and the choice of identifiers by service providers more straightforward.

Cryptography
Several major vulnerabilities over the past few years have underscored the importance of modern cryptographic algorithms. Cryptography requirements in this document attempt to set a firm line for what's needed to securely sign and encrypt. At the same time, the working group tried to make the requirements relatively future proof.

Deep linking
This is an issue that can cause significant frustration to those using federated services that lose track of the intended destination during the login process, and the working group saw this as one that needs to be fixed. The requirements for this aren't complex but serve to remind deployers of something that often gets overlooked, especially when federated authentication is tacked on later.

Support for multiple IdPs
This issue works together with deep linking in most cases. Other profiles and earlier versions of SAML2int mention the importance of IdP discovery. This section stresses that any federated application needs to be prepared to work with multiple IdPs, a limitation of many

applications today.

Logout recommendations
Federated logout is a long-standing debate in the community. The working group, after much debate, created requirements to establish clear guidance. IdPs need to accept a logout request from an SP and need to publish a logout endpoint. What they do with the logout request is somewhat flexible: there's not a one size fits all. The profile also touches on the danger of an SP performing an automatic federated logout as a result of user inactivity. SP support of single logout requests from IdPs is included, but we chose to leave this optional. We feel that our approach will meet the needs of deployers while leaving room for institutional policy.

Logos
Firm requirements around logos have been needed for a long time. Requirements today even differ from one federation to another -- a problem in the era of Edugain. The InCommon baseline expectations provide further necessity for logos. The profile makes some clear guidance for format and size along with suggestions for appearance. The working group tried to be specific while leaving room for artistic interpretation.

In addition to requesting your review of the updated profile, we also encourage you to forward this request to other interested parties. We're hoping for a broad community review.

On behalf of the entire working group, I want to thank you for taking the time to read and carefully consider our proposed updated SAML2int. We look forward to receiving and reading community feedback.

Keith Wessel
Chair, InCommon Deployment Profile Working Group

Attachments:

message-footer.txt 0 bytes