Final Report of the InCommon Deployment Profile Working Group

Document Title: Final Report of the InCommon Deployment Profile Working Group

Repository ID: TI.119.1

Persistent URL: http://doi.org/10.26869/TI.119.1

Authors:

Keith Wessel (editor/chair) - The University of Illinois https://orcid.org/0000-0002-8047-3187
Scott Cantor - The Ohio State University

Alan Buxey - MyUniDays, LTD. https://orcid.org/0000-0001-8217-8379

Judith Bush - OCLC https://orcid.org/0000-0001-6240-4121

Andrew Morgan - Oregon State University https://orcid.org/0000-0003-0677-6988

Eric Goodman - University of California, Office of The President https://orcid.org/0000-0002-5118-3009

Alex Stuart - JISC https://orcid.org/0000-0003-4034-3748

Nicholas Roy - InCommon https://orcid.org/0000-0001-6515-4316

David Bantz - University of Alaska http://orcid.org/0000-0003-0028-9548

Christopher Phillips - CANARIE https://orcid.org/0000-0001-5567-4916

Publication Date: February 14, 2019

Sponsor: InCommon TAC

Introduction

The InCommon Deployment Profile working group was chartered by the InCommon Technical Advisory Committee (TAC) in the fall of 2016. The group was charged with creating a deployment profile that could be layered on top of the SAML 2.0 Deployment Profile, SAML2int, which was planned to receive a much-needed update. The working group would make the needs of the research and education (R&E) community known so that some could be incorporated into SAML2int; the remaining requirements would go into an R&E-specific deployment profile.

This work was a follow-on initiative recommended by the Federation Interoperability working group which created a profile for SAML software developers. The Federation Interoperability recommended a second profile for deployers of SAML-based services and identity providers.

The motivation for this second profile can be found in the Deployment Profile's charter:

> *Operating a broadly compatible SAML-based service or identity provider can be challenging. The standards and profiles that are currently available leave a lot of room for interpretation and customization. While this allows for flexibility, it also results in issues that make interoperating in a federation a lot harder than it should be. While deployment standards exist today, they fall short of solving the whole problem.*

The charter formed the basis for the working group's initial conversations about how to address a standard for deployment. Updating the existing SAML2int profile was the obvious choice for the focus of our work

Process

The working group began by evaluating the issues list from the Federation Interoperability working group; many of the requirements for developers imply configuration on the part of deployers. In addition, many of the issues from the previous working group's list were considered out of scope for their work but relevant for deployers. The group categorized and clarified the issues and added others from personal experience and community input. The result was a list of recommendations for SAML2int, R&E specific issues, federation operator issues, and those not belonging in a profile at all.

The group then tackled a number of tough issues for which requirements were needed but unclear: federated logout, identifiers, XML encryption, and logos. After several lengthy discussions, the group reached and documented consensus on these areas and formed them into requirements. At this point, the group produced a second profile specifically dealing with identifiers. The OASIS SAML V2.0 Subject Identifier Attributes Profile reflects the work done in this area. It attempts to clear up confusion and issues with the numerous federated identifiers available to deployers today.

As the work progressed, the working group realized that, if SAML2int was going to be updated in a timely fashion, they would need to be the ones to do it. The group was depending on SAML2int updates to be completed before an R&E specific profile could be created. Thus, the group produced an updated version of SAML2int for community review and adoption.

The R&E community provided feedback during a consultation period in May of 2018. All of the changes and questions submitted by the community were taken into consideration by the working group during the summer of 2018, and many resulted in changes to the updated version of SAML2int. The following September, the group held two community review calls to discuss responses to the feedback. A small number of additional revisions were made as a result of the community review calls and sessions at the 2018 Internet2 Technology Exchange conference. The completed work is being presented to Kantara to supersede the current SAML2int after approval by the InCommon TAC.

Deliverables

The working group produced the following items during the course of its work:

- SAML V2.0 Subject Identifier Attributes Profile V1.0
- SAML 2.0 Deployment Profile (revised)
- List of R&E-specific requirements for a follow-on working group
- List of federation operator-specific requirements for a follow-on working group

Significant accomplishments

The group calls out the following items that were accomplished in the course of its work:

- Identifiers: To address the large number of identifiers available today, most of which have significant issues or have been widely deployed incorrectly, the group created two new identifier attributes and documented them in a separate profile which is being approved by OASIS SSTC.
- Federated logout: This topic has many options with no guidance. The working group couldn't find a one-size-fits-all solution but instead presented several well-defined options.
- Encryption: A lot of compatibility issues arise from a relying party's requirements around signing and encrypting SAML messages. Clear requirements were created to help to resolve this problem.
- Logos in metadata: After much discussion, a consensus couldn't be reached to create definitive requirements for logos. Basic guidance was created, but the group referred readers to federation-specific requirements. We are deferring to REFEDS to further establish international consensus.
- Error handling: The group discovered a lack of consistency and consensus across our community in use of this element. To resolve this, the profile standardizes the usage of error URLs. Error URLs are important, and with guidance around their use and content, they can be even more useful.

Recommendations to federations for implementing

Several items in the profile will require some coordinated effort by federations for broad adoption, similar to work done to aid large changes in the past such as the move to Shibboleth IdP version 3. InCommon's governance may wish to make some of these requirements part of Baseline Expectations in the future. Items of interest include:

- Changing encryption algorithms
- Adopting new identifiers
- Firming up common standards around logos and enforcing them
- Self-declaration of conformance with the profile for deployments, and publishing list(s) of such deployments
- Work with colleagues in eduGAIN to develop testing tools that cover the relevant profile(s)

Noteworthy differences between Implementation and Deployment Profiles

The working group identified a couple of areas where the implementation profile and deployment profile don't completely align. These are worth bringing attention to, but in the opinion of the group, are acceptable differences.

- Clock skew: the implementation profile is vague on this, stating a reasonable value with a recommended three to five minute range. The Deployment Profile requires a maximum three to five minute range.

Remaining items for R&E-specific, application-specific, federation operator and other work

Several items were identified that would create excellent profile requirements but are inappropriate for one reason or another for SAML2int. Some of these are specific to the needs of the R&E community and belong in an R&E deployment profile layered on top of SAML2int. Others are related to development of federated applications rather than the SAML layer. A small number of items were also identified that would fit well into a profile for federation operator best practices. These items are documented here for consideration by future InCommon efforts.

R&E-specific profile:

- Adoption of the new SAML subject identifiers
- Agreement on logo standards for use in metadata
- Define and publish a standard that declares attributes for use in R&E federations

Federated applications profile:

- Authorization, provisioning and de-provisioning using standard values
- Identifier mapping from asserted identifier into application-specific identifier

- Application support for custom authentication context class references such as the REFEDS MFA profile, including use for 'step-up' authentication and possibly forced re-authentication, SPs must check AuthnInstant
- Configuring attribute release/consumption based on available context
- Adoption of the new SAML subject identifiers
- Development of a "Ready for Collaboration" entity category

Federation operator profile:

- Standardized attribute release requirements for participant IdPs (could get tricky with applications that don't want attributes, for example library /publisher SPs)
- **NOTE: This requirement needs to be better defined:** Dealing with FERPA suppression of attributes for graduate students participating in research projects
- Prevent vendors from charging fees for use of SAML in a multilateral federation context
- **NOTE: This requirement needs to be better defined:** "Lack of framework/contract terms; change controls, support escalation"
- Publication of security contact information for incident response (requirement for support for SIRTFI)

Additional advice for service providers

The group originally added an item to the revised SAML2int that they later felt was advice, not a profile requirement. The item stated that a service provider that requests forced reauthentication should verify that forced reauthentication was performed. While this is a very wise thing to do, it's not firm enough to be required by a profile. Further, it suggests other items that SPs should do. Other items include: verify requested authentication context was satisfied, synchronize server clocks using NTP, and check for attributes in a SAML response rather than granting access based solely on the presence of a successful response. There are certainly others, and these lend themselves to an advanced topics write-up for SP on-boarding. The group recommends that InCommon explore other topics to be addressed in such a write-up and add it to the work of the SP on-boarding working group.

Next steps and recommendations to InCommon

First and most obvious, the working group recommends that the TAC support the revised SAML2int being presented to Kantara's Federation Interoperability Working Group (WG-FI) for review and ratification. Once ratified, we recommend that REFEDS works to integrate the requirements of the revised profile into federation-specific requirements. Even though this group considers our InCommon work complete, most working group members will attend the Kantara working group to represent the work and respond to any community feedback.

As noted above, there are requirements that were left out of this profile that don't apply globally but benefit an R&E specific application. The working group recommends that the TAC charter an effort to create an R&E-specific profile to be layered on top of SAML2int using the above requirements as a starting point.

Many of the requirements in the revised profile need to be widely adopted to be useful. The working group recommends that such items be considered for addition to the InCommon Baseline Expectations. Such candidates might include adoption of new identifiers, upgrading to new encryption algorithms, timely metadata consumption, proper error handling, and compliant logout processes.

The working group recommends that InCommon establish automated tests for requirements where possible. Obviously, many of the requirements can't be tested, but there's benefit to testing and notifying contacts for lack of compliance with those requirements that can be tested.

The SAML 2.0 standard has had a number of errata filed since its creation along with a number of suggestions placed in the SSTC-Jira backlog. The working group recommends that InCommon directs the OASIS SSTC to compile these changes and additions into the creation of SAML 2.1.

The now-final OASIS Subject Identifiers specification creates new identifier Attributes analagous to OIDC's "sub" claim that replace eduPersonPrincipalName and eduPersonTargetedID and all uses of SAML Name Identifiers. As both of these legacy attributes are part of the Research and Scholarship attribute bundle, the working group recommends study of how to evolve the successful R&S entity category towards a future state that encourages adoption of best practices.

Finally, the working group recommends some well-planned marketing and incentives to help InCommon participants achieve compliance. This could involve adding items to Baseline Expectations as noted above, but it also could include a badge or signaling in metadata. As with SIRTFI, metadata signaling could be self-asserted. InCommon might also want to consider a Baseline+ certification; participants who don't meet the extra requirements won't be removed from the federation, but those who do will receive additional benefits. Adherence to many items in this profile might fall into that category.

References

- SAML V2.0 Interoperability Deployment Profile: https://kantarainitiative.github.io/SAMLprofiles/saml2int.html
- Community Consultation Feedback and Responses: https://spaces.at.internet2.edu/x/GA