Final Report - Federation Interoperability Working Group 1

Report to the InCommon Technical Advisory Committee

March 3, 2016

Chair: Walter Hoehn, University of Memphis

Contributors:

Scott Cantor, The Ohio State University

Rainer Hörbe, Identinetics GmbH, Kantara Initiative

Tom Scavo, InCommon

Eric Goodman, University of California, Office of the President

Brett Bieber, University of Nebraska-Lincoln

Nick Roy, InCommon

Barry Ribbeck, Rice University

Judith E. Bush, OCLC

Mike Grady, Unicon

Scott Koranda, LIGO

Introduction

The InCommon Federation Interoperability Working Group (FIWG) was chartered by the InCommon Technical Advisory Committee (TAC) in July, 2015 to help improve interoperability within InCommon and across scalable SAML federations more broadly. To quote the charter[5]:

> When InCommon was created 10+ years ago, it was an explicit goal to keep the bar for membership and operational participation as low as possible. This helped to grow the Federation to its current size. This has also hindered interoperation. Members cannot make any real assumptions about policy, practices, and the supported functionality at other member sites when attempting to interoperate. Both IdPs and SPs suffer from this problem. Areas that are affected include:

1. The functionality provided by a SAML implementation (whether open source or commercial)
2. The sites' policies and architectural choices integrated with their SAML implementation of choice
3. The way that a site configures the overall package to operate within InCommon

> This Working Group is charged with developing both minimal and best practice statements in order to improve the "interoperate by default" situation.

The working group was charged with addressing all three of the identified barriers to interoperability, with an expected deliverable date of the end of calendar year 2015.

The TAC sought working group membership from the InCommon participant community, as well as the REFEDS and Kantara Initiative groups. Active participants included members from the US (higher education, research and industry) as well as EU (higher education, research and e-government).

The group quickly determined that the first point covered in the above charter text (implementation specification) was likely to yield the most impact and is a critical missing piece for use of SAML software in scalable SAML federations. The group worked with TAC to get approval to proceed on a SAML implementation profile to address this need, and proceeded to do the bulk of the content creation through the fall of 2015.

The SAML V2.0 Implementation Profile for Federation Interoperability

The work product of the working group is the SAML V2.0 Implementation Profile for Federation Interoperability [1]. This is an implementation profile intended for use by SAML software engineers and architects as a normative guide for design of their software to meet the requirements of a scalable SAML trust model rooted in multiparty metadata exchange. It is a counterpart to the earlier saml2int [2] work on configuration of SAML software for a scalable deployment (more on that in the next section). Without the implementation requirements documented in this new work, it may be impossible for SAML implementations to meet the configuration requirements in saml2int.

Additionally, it is hoped that this work will be incorporated into federation software test suites such as fedlab [3]. One of the core fedlab team members (also a Kantara WG-FI and eGov member/chair) was an active contributor to the document, and will help shepherd it into the test suite and through the Kantara process (more in "Recommendations" section). In turn, this should serve as a basis for InCommon and other operators to create test tool deployments on which to base other possible means of communicating compliance with this and other profiles, for example, entity category tagging for complying deployments.

Work Remaining

The charter for the group was quite broad, and the group could only complete one of the tasks assigned to it in the time available. The other items that remain to be completed are the second and third items on the charter:

1. Sites' policies and architectural choices integrated with their SAML deployment
2. The configuration of a deployment to interoperate scalably with InCommon

The FIWG recommends the following actions to address these outstanding items:

1. Address deployment issues remaining on the Interop Issues List[4]
    a. Work with REFEDS and the Kantara WG-FI to revise the saml2int [2] deployment profile in alignment with the new implementation profile [1]
    b. or, charter a new working group to identify needed revisions to saml2int [2] and figure out a hand-off that factors in REFEDS and the Kantara WG-FI
2. Charter a new TAC working group to focus on InCommon deployment requirements (using the Interop Issues List[4] as seed material)

Recommendations for Publication

The FIWG recommends that the TAC work with the Kantara WG-FI and eGov working groups to try and achieve consensus around a common profile for InCommon and the e-Government sector. This would increase interest in adoption and provide a long-lived home for the profile in a neutral body that already hosts the "saml2int" deployment profile that was produced by the R&E community. Multiple Kantara participants have expressed interest in this, and Rainer Hörbe has offered to help shepherd the draft through this process. In the event that consensus proves impossible, the draft could still emerge as a Kantara document, or alternatively the TAC may consider other options such as the REFEDS publication stream.

Suggestion: Use Appendix A, Example 3 as the structure / language for IP turnover to the relevant Kantara Working Group(s), from the Internet2 IPR: http://www.internet2.edu/policies/intellectual-property-framework/#ap03

Note: Nick Roy and Ann West of InCommon have a meeting scheduled for Friday, March 4, 2016, to meet with Internet2 legal about the details of such a handoff of IP.

References

[1] SAML V2.0 Implementation Profile for Federation Interoperability

[2] SAML 2.0 Interoperability Deployment Profile

[3] Fedlab

[4] Interop Issues List

[5] InCommon Federation Interoperability Working Group Charter