Test Federation Requirements

Prepared by: Nick Roy
Date: April 18, 2018
Status: Draft v0.2

Goals

1. Create a facility for
    a. Operations and others to test federation components, including metadata creation, aggregation, signing, publication, IdP and SP integrations to be tested
    b. Members of the community (InCommon participants and prospective InCommon participants) to test their integrations in a realistic multilateral federation environment
2. Discourage use of the test environment for anything other than testing (active measures to prevent production-like use)

Components

1. Metadata ingestion and management
2. Metadata signing
3. Metadata publication (aggregates and per-entity)
4. Metadata consumption
5. Test IdP(s)
    a. InCommon
    b. Users
6. Test SP(s)
    a. InCommon
    b. Users

Scope for completion during Phase I: metadata consumption, aggregation and publication
Scope for completion during Phase II: InCommon test IdP and test SP configured with R&S attributes, consent (on IdP)
Scope for completion during Phase III: Solicit a partner organization to develop SAML testing tools for use in the test federation

Metadata Lifecycle (Phase I)

1. Static test fixture metadata (TIER components, test IdP, test SP run by InCommon) persisted in persistent S3 bucket

2. User test metadata submitted via simple self-service interface that accepts SAML 2 Web Browser SSO-compliant metadata, validates it against Shibboleth MDA ruleset
    a. The interface checks and sets some additional parameters in metadata:
        i. entityID MUST be a URL that begins with https://testfederation.incommon.org
        ii. Logo URLs are set with an obvious test logo URL
        iii. DisplayNames are set to “zzzTEST - {submitted display name}”
        iv. A technical contact name and email address are required, and metadata will only be accepted upon positive proof of possession via an activation link sent to user at successful metadata submission time
        v. Up to three arbitrary user-defined entity attribute name-value pairs per entity
        vi. “The usual” set of attributes may be set as requested attributes, with isRequired=true optional on SP metadata
    b. The interface requires users to acknowledge that the metadata is for test purposes only and will age out after 30 days, and that the signing key for metadata may be changed with little to no notice.
    c. The user accepts
        i. If metadata is valid, written to S3 bucket with a 30-day age-out period, indexed by its entityID. Anyone can submit metadata with any entityID. EntityID submissions clobber existing entityIDs in the S3 bucket.
        ii. If metadata is invalid, user is shown error messages returned from MDA, metadata is discarded
3. Every x minutes (depending on speed of our ability to sign), process aggregates metadata in static bucket and age-out bucket (any entityID in the static bucket clobbers any matching entityID in age-out bucket), signs both a test aggregate and test per-entity metadata, publishes the metadata at test endpoints for consumption

Testing Lifecycle (Phase II)

1. User requests test credentials for:
    a. R&S compliant IdP
    b. R&S compliant SP
2. The interface requires users to acknowledge that the credentials are for test purposes only and will age out after 30 days, and that the signing key for metadata may be changed with little to no notice.
3. The user accepts
4. The interface requests a technical contact name and email
5. The interface sends a confirmation link to the email address supplied
6. The user clicks the confirmation link
7. The interface provisions a number of test user principals and associated R&S attributes into a test directory (LDAP, possibly backed by a Kerberos realm)

8. The test user principals are configured to represent typical users with each of the following affiliations per the eduPersonScopedAffiliation controlled vocabulary:
    a. Student
    b. Staff
    c. Faculty
    d. Affiliate
    e. Member
    f. Library walk-in
    g. (No affiliation)
9. The user principals' email addresses are set to the email address of the requesting technical contact
10. The user principals' displayNames are set to the name of the requesting technical contact, prepended with an indicator of which principal they are, e.g. "[affiliate] Steven Zoppi"
11. The user principals' eduPersonPrincipalNames, usernames and passwords are supplied to the requester
12. After 30 days, the user principals are removed from the directory (and Kerberos, if being used)
13. The test SP may be accessed via a well-known URL supplied to the requester. Upon successful authentication at the test IdP with any of the active user principals, the user is granted a SAML 2 web browser SSO-compliant SAML assertion which may be used to access the test SP. Any IdP in the test federation may supply a similar assertion and its users granted access to the test SP
14. The test SP runs a simple web application which dumps all relevant assertion material (all eduPerson and inetOrgPerson attributes in the session) into the browser window in a nicely formatted table, along with debugging info about whether or not the supplied assertion will be sufficient to grant the user access to an R&S application

SAML Test Suite (Phase III)

1. InCommon's community governance bodies (some combination of CACTI, TAC, CTAB, Steering) determine what it means to be "InCommon Certified"
2. InCommon staff develops a program (business model, business processes) to fund and maintain the certification program
3. Internet2 issues an RFP for a development partner to develop and maintain a suite of test fixtures for use in the test federation that address the certification needs developed as part of Phase III (s)1.
4. InCommon/Internet2 staff works with partner to implement test fixtures as specified, and deploy them in the test federation
5. Partner maintains test fixtures and develops changes as requested by InCommon/Internet2 under the terms of the business model and agreement

6. InCommon/Internet2 staff accept applications for certification and receive / act on notices of validation generated by the test fixtures