Project Roadmap

Shibboleth Project Work Packages

The following document track the various work packages within the Shibboleth project.

It provides:

- a high level description of each work package
- whether the project is being worked on now or will be in the future
- estimated completion date of the work, assuming a stable level of developer resources
- the total amount of time, given in person months (PM) each work package is expected to take
- the amount of time, given in person days (PD) per calendar month, individuals spend working on the package
- the relationship between packages

> Note, all work packages related to software products include development, testing, packaging, and documentation within their total effort estimates. Total effort estimates however do not include user support time which is covered by a separate work package.

This document does not provide deep technical details of the work going on in any particular software project but it does link to such information when available.

Comments, suggestions, and discussions regarding listed work items should be directed to the **developer's mailing list**.

Committed Work

The following work items are currently staffed and work is ongoing.

Name	Completion	Total	Depend	Description
Project Overhead and Infrastructure	ongoing	n/a		This work package encompasses efforts to "keep the lights on" for the Shibboleth projects. This includes attending teleconferences, face-to-face meetings, core list emails, etc. Also includes ongoing management of the infrastructure, and basic coordination among the team.
Standards Development	ongoing	n/a		This work package encompasses the effort expended to participate in, and keep track of, specifications from standards bodies such as OASIS, W3C, IETF, Kantara, etc. We have scaled back our efforts here to focus on development work in recent years.
User Support	ongoing	n/a		This work package encompasses the effort spent supporting users of the Shibboleth software through the Member-only support mechanisms or in response to mailing list questions from members. Non-member support is not subsidized and not project time.
OpenSAML-C, version 3, Maintenance	ongoing	n/a		This work package encompasses the effort in maintaining the V3 C++ OpenSAML stack (the xml-security, xmltooling, opensaml libraries). This includes bug fixes, testing, release preparation and distribution. It does not include significant feature work.
Native SP, version 3, Maintenance	ongoing	n/a		This work package encompasses the effort in maintaining the V3 Service Provider product. It includes bug fixes, testing, and release preparation and distribution. It does not include significant feature work.
Embedded Discovery Service, version 1, Maintenance	ongoing	n/a		This work package encompasses the effort in maintaining the EDS, including bug fixes, testing, and release preparation and distribution.
OpenSAML-J, version 3, Maintenance	ongoing	n/a		This work package encompasses the effort in maintaining the V3 Java OpenSAML library and supporting libraries. This includes bug fixes, testing, release preparation and distribution. It does not include significant feature work, as active development has moved to V4.
IdP, version 3, Maintenance	ongoing	n/a		This work package encompasses the effort in maintaining the V3 Identity Provider product. It includes bug fixes, testing, and release preparation and distribution. It does not include significant feature work, as active development has moved to V4.
Metadata Aggregator, version 1.0	2020?			Initial product release of the framework and command line tool. Excludes previously intended Metadata Query Protocol functionality and in-depth documentation.
OpenSAML V4	Q1 2020			Next feature update to libraries, principally focused on cleanup, possibly requirements for more complete SP functionality in Java to support IdP proxying.
IdP V4	Q1 2020	1+PY	OpenSAML V4	An upgrade focused on move to Java 11, Spring 5, and elimination of deprecated features and APIs, and a few new features. More details>>>

Planned Work

Planned projects are work packages accepted by the consortium but which are not yet under development due to lack of resources or unmet preconditions. When committed work packages complete the individuals working on the completed work package will normally pick up the next project from this list.

The following items are listed in order of priority (those at the top being worked on before those at the bottom). The ordering may change depending on available developers.

Name	Completion	Total	Description
OpenID Connect	Java, C++, OAuth/OIDC	2.5PM (Java prototype), 10-12PM (Java comprehensive) 3-4PM (C++ prototype), 16PM (C++ comprehensive)	A GEANT project to implement OIDC natively is on its second official release and will be incorporated into IdPv5 after migrating into our Git repository for V4. SP work unlikely given current resources but in a perfect world might be nice to pull in code from mod_auth_oidc.
IdP Proxy Support	Java, work underway	4PM	Add sufficient OIDC and SAML RP support to IdP to handle proxying use cases without additional software footprint. SAML proxying is planned for IdPv4 and additional protocols will be added later.
SP Packaging Automation	2020	1PM	We need to build an AWS-based process for automating SP packaging, at least encompassing RPM, possibly Windows if practical

Under Discussion

These are projects which have been proposed but which the Consortium has not yet decided to work on. Most estimates here are highly speculative.

Name	Skills	Total	Description
Understanding Shib /SAML Documentation	Tech Writing, SME	2PM	Encompasses the effort to develop a good set of documentation that explains SAML, Shibboleth, and Federations at a conceptual level. The intended audience for the documentation is those new to the subject matter.
Enhanced Product Documentation	Tech Writing, SME	3PM	Encompasses the effort to develop a good set of product documentation that explains features more thoroughly and contextually, with examples, and better how-to material that is task focused instead of reference oriented.
Developer Documentation	SME	3PM per product	Encompasses the effort to develop a good set of developer documentation for extension work on Shibboleth products. Documenting the SP and IdP would be separate items.
Infrastructure Documentation	SME	1PM	We have a lot of infrastructure services, but little formal documentation for them, which will make project transitions much harder.
Packaging / Installation / Deployment	Packaging, Containerization, Installer Tools	2PM	This would span general installer improvements all the way to possible use of container technologies like Docker. Unclear if there's value in a general solution to that, but various groups have asked or have worked on things like this. Likely also ties into TIER work or requirements.
TestShib-NG		2.5PM	This work package encompasses the effort to create a new TestShib software package. The current TestShib's registration system was developed by a number of novice programmers over a period of years. This product would involve producing a more supportable test platform and making it a consortium service. This is like to involve more than just programming, but an ongoing investment in supporting it with more than volunteer effort. Of late, samltest.id seems to have filled this niche well enough.
Expansion of IdP Integration Testing	Java, Installer Tools	2PM	We need more extensive coverage of the installation processes and integration tests across different supported containers and platforms, to improve QA.
Token Binding	Java, C++	2PM	Support for the emergent TLS Token Binding extension in our SAML implementations. This is very uncertain in light of Google at least for now having pulled Chrome support for Token Binding.
IdP User Interface	Java, Javascript		There are various things that the IdP might expose a UI in order to manage, such as: • User-initiated IdP-initiated Single Sign On and Single Log Out • User-initiated persistent ID disassociation • User-initiated removal of attribute release consent • Admin-initiated single logout of user • Admin-initiated reload of selected subsystems or metadata sources

SP Availability in Fedora	RPM packaging		This work package encompasses the effort to produce SP packages compatible with Fedora standards and to get them accepted into the Fedora project. This has unknown implications on Red Hat packaging. This was a request from the Moonshot team.
SP OAuth Implementation	C++, OAuth	3-5PM	The SP supports web service security using the SAML ECP profile in a manner that supports N-tier delegation. OAuth in its typical form is a simpler mechanism that reinvents cookies and works when N=3 (site accessed by browser wants to access another site). The SP could include an OAuth token flow for protecting access to itself, providing another way of hosting web services with attribute-based authorization. In this model, the SP issues tokens to itself, so there are no interoeprability considerations. Either cookie-like bearer tokens or something stronger could be implemented (taking more time), but in practice no clients are likely to support anything stronger.
SAML-ECP GSS-API Mechanism	C++, GSS-API and SASL	10PM	Specification of a browser-less GSS-API mechanism for SAML based on ECP is largely complete with stable drafts available. Completion of the drafts depends on implementation feedback. A mechanism would need to be developed in C++ with C linkage to the mechglue layers of at least MIT and Heimdal GSS libraries. Other implementations, such as Java, would also be useful if possible. Some prototype work on this was done by NCSA staff with ISOC funding. This work item refers to productionizing this code under the auspices of the project, and extending it with additional features.
Confluence /Jira Plugins	Java	mainly some ongoing maint.	Many sites are using various forks of code originally from the project for SSO integration for Confluence and Jira. The code is somewhat maintained for Confluence and Jira. Since the project is running those products and forced to use those plugins, offering officially supported versions might make sense to help defray the pure overhead of running them internally.
Java Service Provider	Java, SAML	8PM	An analogue of the native, C++, SP written in Java. This has been requested for a long time due to the deficiencies so many other SAML implementations have had. It's been parked for a long time, and we had hoped to see good implementations emerge, but that hasn't happened. It may be time to revisit this, especially now that some of the code needed has been fleshed out as part of library work for V3. Some older design thoughts around this are here. There has also been work on a SAML JSR, although the state of that and its soundness are not clear.
Office 365 Integration	Java, WS-Trust	3PM	Microsoft has made documents publically available describing fat-client integration with Office 365 via WS-Trust. They are offering technical contacts to faciitate this work. We have to determine viability and our willingness to adopt non-standard profiles without public change control procedures. This work seems of questionable value now given the SAML support across most of the applications.
OAuth Authorization Service	Java, OAuth	8PM	OAuth 2 introduces an infrastructure component for issuing authorization tokens, essentially similar to some of the eventual goals for SAML. We could add this kind of functionality to the IdP. Neither the demand for this, nor the actual use cases, are very clear at the moment.
IdP One Time Password SMS Authentication	Java		This work package encompasses the effort to add support, to IdP v3, an SMS based multi-factor authentication mechanism. The idea is that after a username/password loginthe IdP would send an SMS message containing a code that would be entered in to a second login page. More Details >> SMS seems to have rightly lost a lot of supporters given its security flaws. Work on other tech probably makes more sense.
IdP Configuration Tooling	Java, Javascript, UI design		From time to time people have requested some form of configuration tooling for the IdP. The suggestions range from command line tools, desktop UIs, and web-based UIs. In general it seems like the most often wish revolve around configuring: • Generate metadata based off of configuration • Add/remove metadata provider - will support file and URL based metadata and digital signature validation • LDAP/Kerberos/Container authentication • Database and LDAP data connectors • Configure release of attribute to all, or a specific, relying party The Unicon GUI is convering a lot of this space at the moment though in a highly abstracted/insulated way through the metadata boundary and the MetadataDrivenConfiguration work.
Security Audit /Review	C++, Java		Various open source projects have undertaken formal code audits or reviews for security issues, and this sometimes is raised as a pseudo-requirement for governmental usage. We have a lack of resources/expertise, and no explicit demand/requirement for this. It would also be costly in time.
Elliptic Curve Encryption	C++, Java	1PM each	Encryption using Elliptic Curve keys is currently not supported by either IdP or SP and is not supported in either of the XML Security Libraries we use. This would entail donating implementations of EC-DH to Apache and then supporting them in our software. Without this work, it's impossible to fully migrate off of RSA keys. Unclear at this point whether this is worth doing or not, and it's not generally supported by other implementations.

Parked/Rejected Work

These are projects which were proposed but were found to either be ill-defined, out of scope, or without sufficient interest from the project members. These items may be revisited from time to time as situations change.

Name	Description
Centralized Discovery Service, version 2	This work package encompasses the work of developing the next major version of the Centralized Discovery Service product. This includes significant internal code refactoring, changes in configuration files to align with the IdP, and production of JSON metadata feed used by the embedded discovery service. After consultation with members, the decision was made to park any work on this codebase and allow the original version to sunset with the V2 Java code base.

IdP Support for WS-Federation	Version 1.3 of the IdP had support for Microsoft's proprietary ADFS v1 protocol. This was not brought forward because it didn't seem to be used by very many deployers.
OpenID Support	Support for OpenID 2 protocol along with Attribute Exchange, PAPE, and Simple Registration extensions in the IdP, SP, or both. There is no use case for this work or real interest from the community. An prototype extension was available for the IdP for 9 months and only one site tried it. OpenID is now obsoleted by OpenID Connect. More Details >>
InfoCard Support	Support for Microsoft InfoCard managed cards in the IdP, SP, or both. There is no use case for this work or real interest from the community. Microsoft has discontinued its delivery of future versions of this technology. More Details >>
Resource Registry, version 1	Various federations have software that devolves management of IdP/SP information to people closer to those entities. SWITCH's Resource Registry is the canonical example of this. People have made requests that such a tool be available from the Shibboleth project. Currently each federation has something that might be considered a resource registry and each is very different so it's unclear that a single code base could ever cover all, or even the majority, of these uses.
Conformance Testing	Kantara (formerly Liberty) does (or did) some conformance testing of SAML implementations against various conformance testing suites, particularly eGovernment profiles that the project has participated in the development of. Vendors have expressed interest in Shibboleth participating at times, though not recently. There is a lack of demand from our community, and unwillingness to devote limited core team resources to the effort. We also don't support some of the features required by the testing, and do support things we think are more important but aren't part of the testing.
SAML 2.1 Standard	This work package encompasses an effort to update and revise the SAML 2.0 standard within the OASIS SSTC. With the project turnover, we feel unable to provide substantial work toward such an effort. The work at the SSTC has essentially been put on hold due to lack of volunteers to work on it.