Shibboleth 3: A New Identity Platform

Over the previous decade, the Shibboleth Project has produced two major generations of software that have seen successful deployment worldwide. With the transition of the project to the Shibboleth Consortium, we are committed to completing design and delivery of a third generation Identity Provider platform that will carry the project, and more importantly our community, into a second decade.

Extensive modularization will provide a more agile platform able to support evolving requirements more rapidly and with less lead-time. More regular, and higher quality, releases will be possible. Custom authentication, user interface, and policy needs will be more readily met with less code and risk to core functionality. Future additions, such as OpenID Connect, will take less effort for the project to add and maintain. Our experience with the software, and the feedback from our community, have been fed into a comprehensive design process that we are confident will lead to a successful product.

Further maintenance and development beyond this release will depend on raising additional funding, which is why organizations using Shibboleth should join the Shibboleth Consortium.

Shibboleth Consortium

The Shibboleth software is open source and freely available, but the project requires ongoing funding to continue its maintenance, development and support activities. Project costs (including support, maintenance, and new development) are currently in the order of half-a-million US dollars per year, but even at this level it is not possible to undertake all of the work in the project plan.

The Shibboleth Consortium has been established to financially support the project, and has received initial contributions from Internet2 (United States), Janet (United Kingdom) and SWITCH (Switzerland) to ensure the delivery of Shibboleth Version 3. However, additional investors in the project are still needed, so NRENs, access federations, research and education institutes, as well as commercial organizations making use of Shibboleth are strongly encouraged to join the Consortium.

The benefits of joining the Consortium are not only that you help ensure the ongoing development and the support of the software to allow organizations to deploy it with confidence, but you will also be able to influence the direction and priorities of the project roadmap. Your support is needed for Shibboleth to continue into a second successful decade.

The Shibboleth Consortium is managed by the Shibboleth Board in accordance with the Shibboleth Charter (see http://shibboleth.net/documents/charter.html). Principal Members are automatically entitled to be represented on the Board, whilst other members are entitled to be jointly represented. The day-to-day activities are managed by a professional manager.

Membership categories and fees are as follows:

Category	Small	Medium	Large
Principal Member	€120,000	€120,000	€120,000
NREN/ Access Federation	€10,000 <=250 IdP+SPs	€20,000 251-750 IdP+SPs	€40,000 >750 IdPs+SPs
Academic/ Non-Profit Organisation	€2,000 <=10K users	€4,000 >10K users	€6,000 >10K users
Commercial Organisation	€4,000 <=€10M revenue	€8,000 €10-100M revenue	€16,000 >€100M revenue

† It is also possible to become a sponsor if you do not wish to join the consortium.

Goals[CW1]

The development team's experience, community feedback, and requests for enhancements and improvements led us to identify several major areas of need:

- Easier setup and customization of the user authentication process, including non-browser-based applications.
- Easier injection of post-authentication processes and workflows, such as user consent for release of data.
- Avoidance of Single Sign-On (SSO) for shared devices, and Logout.
- Support for non-SAML (in particular non-XML-based) identity protocols, such as OpenID Connect, in future upgrades.
- Alternatives to Terracotta for high-availability configurations.

Many of these features have been available in the form of third-party extensions. The team has worked to identify limitations in the current software architecture that are most critical to address for both the project's own ability to deliver such features, but to substantially decrease the effort involved for outside contributors. Growing the community is a key benchmark for success.

Underlying all of these goals is a continued emphasis on standards adherence, and on backward compatibility. The project learned key lessons from the adoption curve of Version 2.0; simplifying the upgrade process and maximizing reuse of existing configurations is a predominant focus.

Authentication

The Version 2 software was the first release to incorporate user authentication into the core platform, so that both federated and local SSO use cases could be addressed by one system. This was successful, but incomplete. As a first attempt, the feature set has lagged

behind other, more mature, software options, and extending or replacing this functionality has been complex.

A key focus in Version 3 is increasing the modularity of this layer so that more flexible requirements can be met out of the box, simple deployments stay simple, and more complex features become much simpler to build. We have decomposed the user interface, credential/password collection, and validation components of the authentication process to make them smaller, simpler, and easier to combine in new ways to meet new requirements.

This streamlining has been extended to the built-in support for non-browser-based applications via SAML ECP so that a single authentication configuration can support both browser-based and non-browser-based applications.

Terms of Use and Privacy Controls

U-Approve, developed by SWITCH, is a popular third-party extension to Shibboleth that adds a workflow for obtaining user consent for attribute release. The design changes will enable a new version of this software to plug into the platform much more readily and be provided as part of the standard release. In addition, the common use cases of presenting enterprise usage terms when accessing a new service, or performing specialized authorization or provisioning steps, will be easily configurable.

Better Control of Sessions

Logout has been a sore point with many in the community since the earliest days of the project. Shibboleth didn't invent SSO on the web, and the practical fact is that logout remains extremely problematic in a federated environment. Whilst this is difficult to change, the development team has explored many of these issues at length with the community and thinks that Version 3 will position us to work more on this. A simple logout solution is already shipping with Version 2.4, and this will be carried forward into Version 3 as a foundation for future expansion of the feature.

Far more practically, Version 3 will provide out of the box support for user- or network-based "opt-out" of SSO, to give users and sites more control over the system's behavior on shared devices.

Beyond SAML

While Shibboleth remains, for the medium term, a best of breed SAML platform, the obvious industry push toward REST- and JSON-based solutions like OpenID Connect is recognized. The current Identity Provider software platform was designed heavily around supporting XML-based protocols and assertion formats.

Preparing for alternatives necessitates a new design that will more easily accommodate alternatives without sacrificing the security and the flexibility of the platform. The intention is to bring a more security-minded focus to newer protocols than will be found elsewhere, but an improved software platform is needed to get there.

Beyond Terracotta

The choice of Terracotta as a primary clustering solution for high availability has not worked out particularly well for the project and we have been evaluating possible directions and design implications from the early planning stages. While the original intent was to move toward a technology called Infinispan as a replacement, recent experience from the community has not been positive (feedback for which we are tremendously appreciative).

With many sites successfully using extensions that allow for robust clustering without shared state, and most commercial offerings focused on client-side storage of state for scalability, those are more productive directions for the next release. Much design attention has been given to ensuring support will be possible for other popular solutions such as databases and memcached.

Upgrades and Compatibility

The transition between Versions 1 and 2 of the Shibboleth software was not a smooth one, and the upgrade path was not simple because of the significant feature changes between them (most especially the incorporation of authentication into the system). With Version 3, there is an understanding of the need for a better upgrade process and a smaller set of new features to accommodate.

The project plan includes a substantial amount of time spent on configuration design and compatibility issues, and there is a firm expectation that there will be significant compatibility for all of the configuration files that sites normally manipulate routinely, such as attribute resolution and filtering policy, metadata sources, and per-site profile behavior.

The most dramatic changes are again expected to be around authentication, but the Shibboleth Project is confident that it can eventually provide either compatibility or tools to migrate most simple deployments.

Readying for the Future

The project plan, a living document, can be found at https://wiki.shibboleth.net/confluence/display/DEV/Project+Planning and delivery of Shibboleth Version 3 is currently planned for the second half of 2014.