UC Trust As a Service

Viewing UCTrust as a Managed Service - Draft for Discussion

Arlene Allen - February 2013

Current Context

UCTrust operates as a loose confederation of UC affiliated IdP's under a generalized agreement of service coordinated within the UC, and the rules of federation stipulated by InCommon, our federating entity. The UCTrust work group has consensually maintained information about its efforts within the UCLA wiki, and has recently begun architecting processes for the smoother onboarding of SP's that are common to all IdP's. Some campuses have chosen to use federation as a mechanism for single signon within their unique campus milieu, and the UCTrust working group has no interaction with or comment on such activities.

While security practices are generally uniform across the UC due to Regents and Presidential policy, privacy standards are more unique to each campus. In the context of federation, an SP may request the release of certain attributes that SP feels to be essential to their service. Each campus may have a different view on Attribute Release Policy (ARP) and thus have differing internal processes as to satisfying each unique SP's request. While the onboarding process for SP's is becoming standardized, there are still no standards for pre-approved attribute release groups.

An SP requiring any particular IdP to be responsive to its needs is, in effect, creating an unfunded external mandate. This is dealt with on a time as available basis, with some campuses having more free time than others.

The net result of the current context is that the SP onboarding may be problematic for the SP simply due to them being unclear on what the IdP's consider easy to implement vs. hard. The IdP's need to design and schedule the necessary changes to their Shibboleth metadata and put them into service. If the SP has any form of SIT QA/QC they wish to perform, it is usually via individual campus negotiations with IdP personnel. The combination of all of this is that it is seriously labor intensive, from a UC view.

Clearly, this has all worked, but it is not a model of efficiency or consistent results or reliable timing.

Principles

If we view the UCTrust cooperative processes as a managed service, it might be viewed as tier 1 / tier 2 type organizations wherein the tier 1 corresponds to those aspects that are centrally coordinated and done once, and the tier 2 remains within the unique to each campus IdP environment.

Any architected solution needs to respect the individuality of each campus IdP in their support of ARP and privacy. Security processes may remain unique, but it is reasonable to assume that outcomes will be similar due to uniform IT security policies within the UC.

For reasons of its own, any particular campus might not be a participant in what is otherwise a UC wide SP purveyor of certain services. This translates to a common architecture, but not necessarily common availability.

Hypothetical Managed Service Possibilities

Since the UC is starting from the position of the cumulative most costly federated identity, any one or combination of the following would reduce overall expenditure. Additionally, some of the options will result in an improved time to completion.

1) The UCTrust working group could consensually determine the definition(s) of one or more metadata groups that corresponded to the various kinds of business-of-the-UC SP's. These groups might be a one size fits all or they might choose to correspond to the security levels required – perhaps low, medium and high. Low, for example, might correspond to an informational wiki. High might be UCPath.

2) The UCTrust working group could take the proposed attribute release lists for the metadata groups developed and pre-coordinate with their campus in whatever internal process they now have.

3) Individual campus IdP's may have a policy that requires local sponsorship of any SP, regardless of whether it is the business of the UC. This would be noted on any profile of that campus as presented to the management of prospective SP's. Since IdP's are generally unaware of sponsors, it would be the SP's duty to create that arrangement with the appropriate campus entity.

4) An existing IdP could take on the role of "Managing UCTrust IdP". This IdP would be the contact point for all SP development, documentation, policy discussion, etc. It would implement any new SP within the context of the aforementioned UCTrust defined metadata groups. The SIT for any new SP with the Managing IdP would determine the content and correctness of the XML used for that purpose. The Managing IdP would make that XML available to all UCTrust IdP members in a secure fashion. Member IdP's would implement utilizing their own definitions and timing. At a minimum, attribute-filter.xml and attribute-resolver.xml would be developed and tested.

5) An enhancement to the Managing UCTrust IdP would be to create a mechanism for automated download of appropriately vetted XML in much the same fashion as is currently done with the InCommon metadata. Each campus IdP could decide whether it wishes to automate the update of such XML or still choose to review it manually before placing it in operation. Since we seem to be able to trust an independent entity like InCommon, it seems reasonable that we could trust our very limited circle.

Other Notes

The Managing IdP could keep the UCLA wiki space in good order, instead of the semi-chaos we have in between the altruists of the moment who occasionally clean it up.

The Managing IdP could manage the various documentation and help processes that we collectively choose to develop. Right now, help is a bit difficult to predict, since it depends on what the SP is willing to do for their customers, and how much they feel the need to pull an IdP into the process. In the general case, problems are almost exclusively cockpit error on the part of the customer's use of federated authentication or customer error in the SP policy and process for initial provisioning of the customer's access. A single source of documentation and process description that all SP's could refer to would considerably limit SP uncertainty and their subsequent communication with the IdP in question.

While overall, the UC saves money with streamlined identity processes, the Managing IdP would take on some additional work. It is not likely a big increase because most of the activity is that which they would be doing solo in any case. That said, whatever the increment is, it would be reasonable to suggest the other IdP's paying a yearly fee for taking these annoyances off the table. Again, it is likely to be a very small number, especially when it is a divide by 9, assuming ten IdP's total.

A structure such as this would also enable potential solutions to some of the UCTrust working group's other vexations such as InCommon Silver IAQ, and the various union namespace across the UC problems and propositions that have arisen over time. Think Sumtotal here.

P.S.

This is a blue sky type of paper and is by no means cast in concrete. It is hoped to be a start in the improvement of UCTrust processes. I welcome open discussion and constructive criticism. I am happy to progressively edit this document if we get traction on any of these concepts.

arlene