Access Management Team

This is the landing page for the Access Management Team for consolidating documentation, meeting agendas/notes, etc.

Subscribe to the CIFER Access Management list at https://lists.internet2.edu/sympa/subscribe/cifer-am

Team Members: Tom B (convener), Scott, Chris, Jacob, Jimmy, whoever Dedra delegates

Current Work Items

- Access Management Functional Model

Summary of subgroup discussions

The access management "chunk", unlike the registries chunk, has existing open source products developed by the HE community with substantial capabilities and adoption: Grouper and KIM. And unlike the provisioning chunk, there is agreement across many projects and applications about the core objects of access management: groups, permissions (triples conveying whether a Subject can perform an Action on a Resource), roles (groups with one or more permissions), permission inheritance by subgroups of a role, making them superior roles, and more. Cf. the MACE-Paccman work.

Hence, the task of this subgroup was not a greenfield exercise in creating a high level design to meet a set of specified requirements, but rather a discussion that started with how the Grouper and KIM products and communities would relate to a larger IdM suite. Thus, the chief difficulty we faced was the overshadowing of established communities, practices, architectures, and implementations. Fear that one of these projects might find itself falling short on its commitment to their established community had to first be overcome.

The way out of that conundrum is the perspective that, although Grouper and KIM have overlapping capabilities, they are in fact complementary and composable, as has already been demonstrated by production implementation of integration technology co-developed by the Grouper and Kuali Rice teams. So in fact these two project teams have already demonstrated the kind of coordinated approach to meeting shared requirements and developing complementary technology that is the essence of the overall OSIdM4HE approach.

That integration was facilitated by substantial work previously done by the Rice team to design a set of service interfaces that together cover a wide range of access management needs by Kuali applications, so that that work should not be duplicated by each Kuali application team, and so that adopters of multiple Kuali applications should not face the burden of operating distinct access management services for each Kuali application. Do it one way that works for all.

Obviously, many applications run by HE are not Kuali applications, they are not designed to be composed with the KIM service interfaces, and so there remains the problem of integrating their access management needs with enterprise services in a way that is valuable, but that cannot approach the degree of integration achieved by the suite of Kuali applications with Rice, built with a common architecture, enabled by coordinated governance and shared resources. Many non-Kuali applications incorporate proprietary access management capabilities. These must be accepted by each enterprise as givens of the enterprise access management problem. This is a primary high level requirement of work in the access management space, and is what drives the Grouper project's strategy of providing an ever larger array of integration technologies that enable the core objects of access management to be managed in a common access management system and instantiated in an ever larger set of applications.

Recommendations

Recommendation #1
Use the KIM service interfaces as the starting point for defining how core access management objects are communicated between systems in the OSIdM4HE suite, and enhance them as may be needed over the course of implementing integrations between elements of that suite so that at all times they represent the current service contract for core access management objects.

In particular, the Grouper and Rice projects should plan to build additional integration technology to enable the full range of core access management objects to be communicated between them.

More generally, the access management subgroup suggests to its peer subgroups that the KIM service interfaces be the starting point and stalking horse over time for the service contract needed to integrate with IdM registries and with provisioning systems. This would likely result in new types of service interfaces being added to those already in KIM, in addition to enhancing some of the existing ones.

Recommendation #2
The Grouper and Rice teams should adapt their existing means for vetting requirements, producing corresponding updates to their roadmaps, and eventual design and implementation, to recognize when a requirement impinges on the KIM embodiment of the service contract for core access management objects. Further, they should create a venue and methodology for coordinated review of such requirements and determination of complementary design and implementation in their roadmaps.

Although this requirement is scoped to just these two projects, we suggest that this venue for coordinated review of shared requirements, potential enhancement to the KIM service interfaces, and determination of complementary design and implementation, should extend to other projects that become part of the OSIdM4HE effort. In effect, this is one venue in which cross-cutting integration needs are managed. This one is focused on on-going maintenance and enhancement of the KIM service interfaces. There might be others engendered by distinct integration needs among the suite of OSIdM4HE projects.