UC Merced Migrating our current Identity Management registry into midPoint

-John Kaminga, University of California - Merced

Our current IdM system stems from migrating off our old Waveset IdM into MIM (Microsoft Identity Management) with our business logic implemented in Java and an Oracle Database for the person registry. We have 2 main systems of Record, Banner for our student and applicant population and a UC-Wide Peoplesoft system for our employees. We also have a UI built on Angular and using REST to connect to the Oracle back-end. The UI allows admin users to create and edit accounts and allows users to claim their accounts and reset their passwords.

We are looking to use midPoint as our Person Registry. At TechEx 2017, we were very interested in learning about midPoint. When I heard that it had a built-in connector for slack, I was excited because we use Slack. However, when I saw the demo it occurred to me that we want to minimize our downstream feeds from IdM. Preferably, we only want our Identity Management system to send data to Ldap/AD and ODS. Any system should be able to get the data it needs from those systems.

In the past, before my time, the philosophy seemed to be if some department needed student data they went to the Student Information Systems team and If someone needed staff data they went to the Business and Financial team. But, if they wanted both they went to the IdM team, so unfortunately, we ended up with many data feeds from the IdM system to downstream systems, most of them nightly feed files. This became a nightmare to maintain and took up more and more of our developer's time.

We've made a very determined and conscious effort to stop feeding downstream systems from the Identity management system, by sending them to the Data Services team ODS if they need any more data than what's in Ldap/AD. This has allowed us to concentrate on populating our Ldap/AD with only user and access data.