Carnegie Mellon "Accounts Receivable" as a Service

CMU is working with a SAAS vendor to outsource its student accounts receivable functionality but integrate that functionality into its existing Student Information System. Integrating services from many vendors is our core strategy for constructing a new Student Information System. The AR service come with an existing authorization model that has to be integrated into the overall SIS - that model being roles and business rules. CMU is permitted to assert roles as part of a SAML assertion but the fine grained business rules are handled by a UI that exists as part of the service.These rules determine what various roles can do against resources. There are several problems to be solved.

1. The roles namespace in the AR service is not the same as the roles namespace in the overall SIS
2. The AR service keeps no PII data at rest and so everything has to be provided in either the assertion or via a call-back service
3. CMU prefers a more dynamic (subject, function, qualifier) model but the vendor is concerned about the performance of a CMU resident authorization service and would like a local copy.
4. A role based model doesn't easily support delegation in anything but an entire role

Building an application our of SAAS services is a strange sort of federation. As time goes by I believe we will see all the usual access management models (shared directory, authorization assertions passed with each service call, provisioning each service via a privileges metastore).