Streamlining the Admissions Process for Prospects, Service Providers, and Higher-Education Institutions

Streamlining the Admissions Process for Prospects, Service Providers, and Higher-Education Institutions

The Postsecondary Electronic Standards Council Electronic Authentication and Authorization task force and InCommon have partnered with the CollegeBoard and ACT on a pilot project to demonstrate the advantages of having a 3rd party Identity Provider coordinate and register identities on behalf of and to the benefit of participating admissions-related service providers. This document describes how such an arrangement might be established and executed. The alternative case describes a process that simplifies the procedures high school students who wish to enroll in higher education must go through and saves time and money for the participating institutions.

Background

When a high school student prepares for college, there are a variety of steps that must be completed. The student will likely take one or more of the college entrance exams administered by the CollegeBoard (SAT) and ACT as a senior or junior. They may apply for Federal financial aid using the Free Application for Federal Student Aid (FAFSA), administered by Department of Education. Finally, they will apply online, either via the CommonApp or various school-specific online application portals, to one or more institutions of choice.

Each of these services has their own authentication and authorization system and related credentials. A student must apply for separate accounts for each and maintain unique usernames and passwords for each. Typically, 25% of the pool of applicants are accepted and ~~--to say it another way --~~75% of the individuals with these institutional credentials never use them again.

Data comes into the school for each applicant from a variety of sources. When student applications, letters of reference, test scores, and FAFSA funding information arrives at each of the schools involved, the applicant has to be matched to each set of test scores and their financial data at each school.

An Alternative

A prospect decides to take a SAT test as a senior in high school. She finds the College Board site and clicks on a button labeled “Get an AdmitMe Id” after reading how it can enables her to use one user id and password for all her interactions with potential campuses, test services, FASFA and the like during the admissions process. What a convenience!

After clicking on the AdmitMe icon, she’s redirected to a site that’s branded with the AdmitMe Id as well as the College Board logo. She reads the instructions and learns that she just has to provide a small set of her information here to get an AdmitMe credential set. Once she goes through the process, she’s redirected back to the CollegeBoard site and uses her AdmitMe to log in and sign up for the SAT. Next, she goes to the ACT site and clicks on “Login in with AdmitMe” and because she’s leveraging single sign-on technology doesn’t have to re-login. She then surfs to Georgetown’s admissions page and signs up to get information, again without logging in.

The prospect appears at her SAT test time with her ticket to get in along with her picture id that verifies her address on record. The test proctor reviews her information, documents the identity-proofing event and enters it into the CollegeBoard database. CollegeBoard then runs a script to update the AdmitMe database with information about the identity-proofing event. This could elevate her credential to a federally approved high quality credential.

When she brings her ACT exam ticket to the exam site, the process is similar to when she took the SAT. When the proctor exams her admissions ticket and photo ID, an entry documenting this process is made in the databases, which is automatically promulgated to the AdmitMe identity store. This extra vetting of her identity strengthens her credential even further.

Several months later, the prospect decides to apply to schools. She goes back to Georgetown and clicks “login in with AdmitMe” which she does. In the background, AdmitMe sends information to Georgetown about her credential strength, so the institution now has a higher level of trust that her identity online matches the physical person. She then applies to Georgetown. In the background, Georgetown is able to automatically provision access to applicant-specific web pages and an official Georgetown email address for her. Later that day, the prospect collects the information necessary to apply for financial aid and uses AdmitMe to log into the Department of Education FAFSA site. FAFSA’s exhaustive identity verification process is helped by a high quality introduction using the AdmitMe credential, and the AdmitMe credential is then further enhanced by FAFSA’s verification process, again improving the quality of the prospect’s credentials.

After the application is done and considered, Georgetown sends the final information about the financial aid award and invitation to attend the school to the prospect. She uses her AdmitMe account to log into Georgetown and view her SSN and related information, as well as her award package. Georgetown’s financial aid director is pleased to know that the prospects are vetted and proofed---it reduces their risk of fraud and identity theft substantially. And Georgetown’s admissions officer is relieved since AdmitMe service providers all use the same unique identifier for the individuals with accounts, the prospects SAT and ACT reports are identified with their AdmitMe identifier and can be matched up to her record with no headache. What a timesaver!

In the model discussed here, a student will enroll to receive their credentials via one of the participating organizations offering services. It makes no difference which organization they visit first, since all the organizations will use the same enrollment process and tools supplied by the 3rd party provider. In the case of the fictitious “AdmitMe” provider, only enough identity data to use for matching is gathered---nothing related to academics or specific services are asked for. It is just an identity/SSO solutions provider and a repository of information relating to the strength of the credentials that it maintains.

In the background, this is accomplished by setting up a single common identity that uniquely identifies this applicant to all parties. As the student completes the sign up for services at each participating organization's site, additional information will be collected, but in each case this information, stored locally by each organization, is tied to the unifying influence of the 3rd party Identity Provider and the single identity credential.

The one requirement is that they all must trust each other and interoperate. The trust infrastructure is proposed to be the InCommon Federation (incommon.org) which establishes common technology based on standards (SAML), policy, and business operations that participants adopt to share services with each other.

Corporate Partner Benefits

The participants have two roles in federated authentication. One is as a registration authority (RA), where they will provide an entrance ramp to the third-party SSO provider, as well as provide information about the assurance of the identity. The other role is as a service provider, in which they will have a business relationship with the students, the schools, and sometimes each other, to provide services for fees. These organizations are already doing the work of maintenance involved in managing credentials, including password resets and weeding out multiple occurrences for the same individual. Being able to pass these responsibilities off to a 3rd party will reduce expenses. Being able provide applicant data that is keyed to a specific applicant will improve product.

Campus Benefits

In the scenario above, the prospect is identity proofed when she takes her SAT exam. Under this new system, the recording of this event will be maintained in the third-party database. If the student takes a second exam, either with the same or competing service, their ID is checked again, and another record is made, and the credentials are even more valuable. If FAFSA participates, their vetting process can be recorded at the Identity Provider. Once again the credential becomes that much more valuable. When the prospect then uses this same credential to apply for entrance into a higher education institution, the campus is pretty sure the identity is who they think it is because of the identity proofing that has been captured. Having the prospect view sensitive financial aid information is no longer an issue.

The institution is also able to confidently match a prospect with all the documents generated by and for the prospect. The unique ID stored at the 3rd party identity provider will automatically match each document to the prospect.

Finally, the institution will not need to manage accounts for tens of thousands of prospects (in the case of the large institutions) who will never attend the school or have a further relationship.

End-user/Prospect Benefits

From the prospect's perspective, nothing really changes, except the student only has one username and password to remember. No matter which participating site they visit, it will carry the branding of third-party identity provider.

Summary

This scenario can be grown over time but has at least the following 4 benefits for the institutional and corporate service providers:

- Outsourced user identity management and authentication, including password reset.
- Ability to leverage credentials that are at a much higher level of assurance than we have today.
- Matching up of information about individuals using the third-party identifier.
- For your users, it's single sign-on for their entire admissions process.

How do we get there?

Contacts:

Arnie Miles: adm35@georgetown.edu

Ann West: awest@internet2.edu