OpenID Connect is an “interoperable authentication protocol based on the OAuth 2.0 family of specifications”—that is, it uses the standardized message flows that OAuth makes available in order to provide identity services. It does this by building “on the success of SAML2 Web Browser SSO.” Essentially, OpenID Connect lets “app and site developers authenticate users without taking on the responsibility of storing and managing passwords in the face of an Internet that is well-populated with people trying to compromise your users’ accounts for their own gain.”

OpenID Connect is the third version of OpenID technology; it improves on earlier versions in that it is more developer friendly, removes some design limitations, and expands the number of places where it can be used. It can be used by native and mobile apps, as well as by web-based applications.

Whereas OAuth is limited to authorization, OpenID Connect goes one step further to allow for authentication—that is, ensuring that the person accessing your apps is who he says he is. OAuth works using access tokens, while OpenID Connect uses that plus an ID token that contains information about the authorized user. In addition, OpenID Connect standardizes some areas that OAuth leaves up to choice, e.g., dynamic registration of clients, which “makes it easier to write code that lets the user choose between multiple identity providers.”

Importance to Higher Education

Higher education does not exist in a vacuum. Our institutions “need to use the same federation protocol” as large consumer identity providers. If commercial website and app developers use OpenID Connect to provide content and services (for instance, course material or e-mail) to higher education users, we may need to be prepared to work with the protocol.

Some discussion surrounds whether OpenID Connect will replace SAML as the dominant protocol for single sign-on authentication. Thomas Scavo of InCommon, which is based on SAML, has indicated that “all the major e-mail providers either do (or will) support OpenID Connect” and stated that, in anticipation that this support will only grow, “we’ve started to leverage social identity and experiment with OpenID Connect,” including migrating the Internet2/InCommon Google Gateway to it. Gluu has a Shibboleth
plugin that allows for simultaneous SAML and OpenID Connect sessions. Many higher education institutions currently use Shibboleth and InCommon; knowing that this change may be coming will be important.

**Current Landscape**

The OpenID Connect standard was finalized in February 2014. Higher education institutions can implement OpenID Connect by outsourcing this work, using existing libraries or plug-ins, or implementing the protocol themselves. It has been adopted by major players, such as Google, Microsoft, and Salesforce. As more and more of our services are being accessed over mobile devices, making sure that the services are being accessed in a secure fashion is essential.

That said, from the perspective of a campus identity management (IDM) office interested in deploying an identity provider solution, OpenID Connect effectively duplicates the existing Shibboleth/SAML deployments predominantly in use. In addition, many of the supporters of OpenID Connect (e.g., Google and Microsoft) also support SAML. Nonetheless, OpenID Connect is a technology that campus IT planners, especially IDM offices, should track closely.

![Figure 1. Results of the 2015 Top 10 Strategic Technologies survey, when asked about OpenID Connect](image)

**When You Should Expect It**

OpenID Connect is already in use, as is OAuth, on which it is based. The outstanding questions for higher education are the extent to which institutions need to be aware of its use in the third-party applications (e.g., e-mail or LMS) that we provide to our users, and whether we should begin to implement it in our own native apps and website development. The answers to these questions depends on the environment; if OpenID Connect is employed on a wider basis, and if website developers “create a lot of compelling content that universities want, there will be a clear business case for adoption.”

OpenID itself is still undergoing rapid change, but, depending on the rate of cloud service adoption in higher education and of protocol convergence among cloud services, OpenID Connect adoption in higher education will likely increase in the next two to three years. Application developers who are currently looking to serve higher education should consider developing solutions that support modular/swappable authentication/authorization approaches, with SAML being the default protocol for now.
Reviewer
ECAR would like to thank Albert Wu, Senior Director, Information Management Services, UCLA, for his very helpful and significant feedback to this paper.

Notes
1. See “OpenID Connect FAQ and Q&As.”
2. See “The Rise of OpenID Connect.”
3. “OpenID Connect FAQ and Q&As.”
4. This is one distinguishing characteristic between OpenID Connect and SAML, which is limited to web-based apps.
5. See “Why Use OpenID Connect Instead of Plain OAuth?”
6. See “Is OpenID Connect on the Roadmap?”
8. See “Gluu Releases Shibboleth Plugin for OX to Enable Simultaneous OpenID Connect and SAML Sessions.”
9. See “The OpenID Foundation Launches the OpenID Connect Standard.”
10. “Is OpenID Connect on the Roadmap?”