HOCKINGS: But at the end of the day, the question really for enterprise is what level of entitlements that these users should expect to get once they do sign up using a BYOID service or approach. And this means the enterprise will need to consider this authentication mechanism along with the other authentication mechanisms that they traditionally provide to their consumers and provide access rights and policies surrounding this.

[ MUSIC ]

POWERS: Welcome to This Week on developerWorks. I'm your host, Calvin Powers. You know, the consumerization of IT has led to this movement called the Bring Your Own Device movement where people want to bring their personal devices into the workplace.

But a lot of folks aren't familiar with another trend where they want to bring their own identities to the workplace. We're going to talk about this on this episode of This Week on developerWorks, and to help me out, I have invited two of IBM's identity and access management experts to join us.

First we've got Chris Hockings. He is an open group distinguished IT specialist based out the IBM lab in Gold Coast, Australia. Chris, welcome to This Week on developerWorks. Tell us a little bit about what you do for IBM.

HOCKINGS: Yes, I've spent the last 10, 15 years working with our clients within Asia-Pacific on some of their business requirements around access management. I continue in that role evangelizing a lot of our access and identity management solutions to realize those benefits....those business benefits.

POWERS: And our other identity and access management expert that we have with us today is Jenny Wong. She is also based out of the Australia Gold Coast lab. And I like to think of her as the famous person behind our developerWorks Access Manager and SharePoint integration series. Jenny, welcome back to developerWorks. Tell us a little bit about what you do for IBM.

WONG: Hi, Calvin. Thanks. So, I work at the Gold Coast lab in Queensland as a software engineer in a local team here, mainly focusing on pre-sales and post-sales engagements, doing integration work for our access management and identity management products.

POWERS: Jenny, let's start with you. Tell folks exactly what you and Chris mean when you use the phrase "bring your own identity."

WONG: So, bring your own identity -- or, otherwise short as BYOID -- is a concept where Internet users can use their preferred or existing credentials that they have to act as a service that is offered by a provider.

So, if we consider a simple example, is let's consider a company Internet facing Web site such as an online shopping Web site or maybe a banking site, where it provides users the opportunity to use their social media accounts such as Google, Facebook, Yahoo! or PayPal or other credentials that they have to register or authenticate to that Web site to access the service that is available by that Web site.

So, by selecting that option of bring your own identity, the users don't need to record any authentication credentials for the resulting service. From the consumers -- or, maybe we could say the end user perspective -- it offers them the convenience to reuse credentials that they already have and to access services on the Internet-facing site. From a business's perspective, such approach speeds up the delivery of the service on to the end user.

POWERS: It seems like such a natural thing to do because it means I, as an end user, I don't have to remember yet another password. So, of course, I would love to be able to reuse those credentials and bring my own identity to the banking service or whatnot. But I guess the devil's in the details. Chris, why don't you kind of walk us through some of the challenges?

HOCKINGS: So, the BYOID challenges are similar to those that many of our enterprise customers have solved with their B2E situation where employees take their identities from internal deployment and consume cloud services that were on-premises services traditionally.

But it's kind of the opposite. You know, as a consumer, what I want to do is to enroll in services that are being provided by an enterprise, a little more seamlessly from me having to provide identity checks, more onerous ones.
Many financial institutions are considering these kind of channels as a way to bootstrap identities into their enterprise that they don't traditionally have relationships with. So, for example, a financial institution may be looking at ways to provide better financial calculators or mortgage calculators, financial planning tools for those people who are willing to adopt this kind of bring your own identity type situation. This gives the enterprise a much broader set of options for bringing these identities into their organizations and perhaps creating additional revenue opportunities.

But at the end of the day, the question really for enterprise is what level of entitlements that these users should expect to get once they do so not using a BYOID service or approach. And this means the enterprise will need to consider this authentication mechanism along with the other authentication mechanisms that they traditionally provide today consumers and provide access rights and policies surrounding this.

Of course, in addition to that, you know, these enterprises need to understand the range, the plethora of open standards that the social or the mega social and cloud providers actually support so they can seamlessly support those without having to keep adding these authentication mechanisms or registration processes to their online services.

POWERS: There's just a whole suite of standards that are coming together to enable these types of scenarios. Do you want to run through some of those standards for us just real briefly?

HOCKINGS: Yes. There's been the standards...the open standards space has been real interesting the last three to four years with the emergence of social and cloud. What we used to have to do with open standards is we used to have to go to events and perform interoperability style situations with our other vendor partners.

What's happening is that these standards are becoming much more simple to consume for enterprise such that these interoperability events are in some cases not absolutely necessary. They've also simplified the way that two parties can collaborate using these open standards by reducing some of the relationships that have to exist in order for those to occur.

Now, if I think of the BYOID situation, there's a few different standards that kind of follow that pattern of emergence, one being XAML, which some of your listeners may be familiar with, which was one of our first federated single sign-on protocols. This kind of relied on parties getting together and sharing some relationships to support things like just-in-time provisioning and federated single sign-on flows.

Then came OpenID, which limited, or I guess, reduced some of that onerous...that burden on the two parties from entering some agreement. So, you could effectively with OpenID interoperate with your chosen identity provider without the service provider necessarily having a relationship with that identity provider.

And thirdly, the latest is the OAuth standard which is a delegated authorization standard which can be used in a way, which we show in the article, in a unique way to bootstrap registration flows and also then authentication flows. So, those are the three that you'll see in the article, in the publication, of interest.

POWERS: That's right. So, I wanted to talk about the article that you and Jenny just recently published. Folks can get to that article at ibm.co/howtobyoid. That's ibm.co/howtobyoid. Chris, walk us through what that article and its best practices covers.

HOCKINGS: First of all, introduces these standards and their relevance to the BYOID standard and the ones that I've previously mentioned on this recording, and then kind of describes what our major...or what the major social and cloud providers support.

We then kind of go into some details into how you can integrate those standards into both a registration and an authentication flow using our IBM Security Access Manager products. You know, of course when we think of our enterprise customers, we think of them wanting to have some authentication assurance, some closed loop provisioning, those types of things.

And we talk about how to either seamlessly provision these accounts without user names and passwords and also to ingrate with our IBM Security Access Manager user self-care products to provide the ability for the end user to set passwords and other attributes that maybe used later by the enterprise.

The Access Manager product in this demonstration shows some incredible flexibility in being able to support the user self-
care flows, the authentication flows represented by these standards as well as, you know, some of the ability for us to support other standards and flows which reduces the complexity in today's deployments of multiple point products.

POWERS: You know, nothing drives a point home like having some actual running code for people to look at. And to that end, Jenny has put together a demo video. You can see that at ibm.co/byoiddemo. That's ibm.co/byoiddemo. Jenny, walk us through what people will see in that demo.

WONG: So in the demonstration video, what the audience will see is it will showcase user self-care scenarios that can be achieved using IBM security products, primarily focusing on the onboarding process for end users in a business enterprise environment.

So, it will demonstrate a standard self-registration scenario and then follow on to showcase how an external Web site user can easily self-register and authenticate to the enterprise side using a popular social network provider such as Facebook.

POWERS: Jenny, thanks for that. And I'm sure folks will feel like they're really making this vision of bring your own identity real for them when they see it implemented with real products and real code. So, thank you for doing that, and thank you for sharing that with developerWorks.

So, finally, Chris, if folks get fired up and they want to get started making bring your own identity real for them and their enterprise, what's the best way for them to get started?

HOCKINGS: I would be...I would put a plug in for developerWorks. This site has a lot of assets for them to get started with our products and technology. But obviously the IBM Web site under www.ibm.com/security offers a landing page where you can navigate to the different solutions.

You know, these offerings that we're talking about here are what's known as part of the pillar of people within our security strategy blueprint. So, try to, if you see those terms, then navigate your way to the access management section and speak to your local IBM folks to get engaged with people like myself and Jenny.

POWERS: Once again, that's ibm.com/security. You can contact the security folks by e-mail or by online chat, and they'll be glad to help you get started making bring your own identity real for your enterprise. That's all the time we have for this episode. Don't forget you can get all the links for this episode at ibm.com/developerworks/thisweek. All right. We'll see you next week on developerWorks.

[ MUSIC ] [END OF SEGMENT]