

Eduserv's Vision for AIM in 2008

Ed Zedlewski, CIO at Eduserv, asks if federated access management is the end game for access and identity management, or just a stepping stone on the road to user-centric identity management.

Blurring the Boundaries

As technology becomes increasingly integrated into our daily lives, at home as well in our education and working lives, it's little wonder that we are becoming more demanding when it comes to the tools and resources available to us. It has been widely reported that technology provision now plays an important role in a student's choice of university, and employees are demanding the same technology at work as they're familiar with using at home.

But blurring the boundaries between consumer technology and professional and academic technology is not just about businesses and education institutions adopting all the latest gadgets; equally important is the software and user-interfaces available to students and employees, and the way in which they can access online resources and manage their online identities at school, college, university and in the workplace.

The proliferation of social media, such as Facebook and MySpace, means that most individuals have developed their own online identity and their own expectations of the online user experience before they even enter further and higher education, let alone the workplace. So what is being done to ensure that access and identity management (AIM) evolves to keep pace with consumer demand and increasing fears regarding ID theft?

Multiple Identities

Today, each time a consumer, student or employee wants to subscribe to a new online service, they are forced to create yet another online identity, accustom themselves with another authentication process and provide reams of personal information that are then used as password prompts that fraudsters could easily crack.

The result is that the average individual today has tens of online identities, for anything from online banking to accessing a hotmail account, each managed independently with a separate username and password. This means that we either choose usernames and

passwords that are easy to remember and therefore easy to guess, or we resort to writing them down – an obvious security risk.

From a content providers' point of view, the current approach to managing access also causes a headache in terms of the resources needed to manage individual authentication systems. If each user has a separate online identity for every service they access online, then every service provider must individually manage authentication and related customer services.

Federated Access Management

An approach that is now being taken, but so far slow to take off outside of the education and health sectors in the UK, is federated access management (FAM). A federation is a group of identity providers and service providers that share a set of agreed policies and rules. In the case of FAM, these rules and policies relate to the authentication of individuals' identities in order to grant access to online resources or services.

The UK education sector provides a good example of FAM in action. The JISC (Joint Information Systems Committee) and Becta founded the UK Access Management Federation (UKAMF) in November 2006 as a structure and legal framework that enables authentication and authorisation across different institutions and service providers, ensuring that students have access to all the online resources they need through one single username and password.

The government is also making moves in this direction, with plans to enable citizens to create a single online identity that would give them access to all kinds of public services, from paying council tax to arranging waste collection.

An example of how FAM can be applied in the commercial world is where banks form federations with other related but non-competing service providers, such as insurance brokers or financial service providers. In this case, users could access each of their services through any one of their websites, using the same username and password each time.

The advantage of FAM from the end-user perspective is clear; as more and more federations form, consumers would soon be able to reduce the number of passwords they need to remember and would only need to visit a limited number of online destinations to access the majority of services they need. From the service provider's point of view, the advantage lies in the ability to build trust and loyalty amongst their customer-base by providing customers with access to a broader range of online services, and in sharing market information and customer

relationship management with other federation members. They may also see a reduction in the administrative burden associated with managing password reminders as customers have fewer passwords to remember, and therefore fewer to forget!

Despite the benefits, a major barrier to FAM in the commercial sector is establishing trust and a shared understanding of language and terminology in a traditionally competitive environment. How can private companies trust one another's systems to accurately authenticate that a consumer is who they say they are? Who accepts liability when things go wrong? What's more, it may be difficult to find a single organisation prepared to establish and manage the federation on behalf of the other members, in the same way that JANET (UK) manages the UKAMF on behalf of the JISC.

User-Centric ID Management

It is not clear how quickly FAM will take off in the commercial sector (if at all), but it will certainly be the main focus for AIM in the education sector throughout 2008. However, it's unlikely to be the end-game.

The introduction of technologies such as OpenID and Microsoft CardSpace, which enable individuals to create and manage their own online identities, signals a growing trend towards user-centric AIM. Consumers may begin by using these technologies to manage their identities for social networking and eCommerce purposes at home, but how long will it be before they start expecting to be able to use the same online identity to gain access to online resources at schools, colleges, universities or in the workplace? This is not to say that access management federations will be made redundant, but rather that they will no longer need to issue and manage user identity information, but rather grant access to services based on the authentication of their existing identity claims and validate those claims a user makes about themselves from authoritative third parties.

Such a user-centric approach to AIM means that users get to retain control of their personal information, choosing what level of information to pass on to each different service provider they interact with. For example, a user could create one set of claims about their identity for accessing local government services that might contain his or her name and address, another set for accessing health services that would only contain his or her NHS patient number and another for eCommerce purposes that would contain his or her credit/debit card details.

If the main benefit of user-centric AIM to put the end-user in control over their personal identity information, then the biggest barrier to service providers adopting this model is the fear of 'losing control' over

the identity authentication process. It requires service providers to enlist a great deal of trust in the technologies behind it. Yet, that same barrier is in fact the main benefit to service providers as the 'loss' of control equates to an evasion of responsibility. The duty of care to ensure that a customer is who they say they are would no longer lie with the banks or other service providers, but rather it would become the consumers' responsibility to ensure, with the help of technologies like Microsoft CardSpace, that their identities are protected. Thus, all the headaches associated with identity management and authentication would be removed and service providers could focus on their core business.

2008 and Beyond...

It is clear then, that a move towards user-centric identity management would ultimately turn the landscape we're accustomed to on its head. As such, it is not likely to take off until all the questions are answered and barriers removed. Federated access management is likely to remain the focus of debate for at least 2008, but any organisation investing in providing access to online resources needs to make sure that its investment is future-proofed by using established open standards. This will ensure that organisations can take advantage of new developments based on open standards that deliver a user centric approach further down the line.

By 2010, end-users will be controlling the release of their own identity claims for anything from arranging for their rubbish to be collected to buying car insurance online. There will be little distinction between their online experiences at home, in education or in the workplace.

###