

This story appeared on Network World at  
<http://www.networkworld.com/newsletters/dir/2006/0731id2.html>

## Making ID mgmt. convenient to users - no matter what device they're using

### Consider users when thinking of identity management

[Identity Management Newsletter](#) By Dave Kearns, Network World, 08/02/06

The end of the firewall is something I've talked about before in this newsletter as well as, more extensively, in the Windows Networking newsletter (see "[Time to rethink the term 'firewall'](#)"). When the network becomes borderless, you can no longer police the border. That topic came up in a conversation with Steve d'Alençon, senior vice president of marketing at [Encentuate](#), when he said: "Enterprise perimeters are disappearing."

He went on to explain that he meant that end-users access corporate networks and resources from a wide variety of end-points and access paths, such as personal or shared workstations within the office, PDAs of many varieties, kiosks, home office computers, virtualized remote access terminals and more.

But not only are people accessing the network from multiple places, platforms and paths - the experience on each of those can be very different. Mobile users can be users who move within the building or campus or those literally on the road for a business trip or sales call. They receive an inconsistent user experience to access the systems, applications and information they need to perform their job. According to d'Alençon, this heterogeneous environment is a trouble spot for IT to provide a consistent end-user access experience, consistent identity, security and access control, workflow policies across end-points and compliance tracking.

Well, that's true as I think we all can agree. But is it relevant to our identity management discussion?

It's relevant, d'Alençon said, because a "user-centric end-point Identity and Access Management (IAM)" approach is the only way to deliver balance. User-centric end-point IAM effectively solves the business issues of multiplying end-point devices, inconsistent end-user access experience, threat of a security breach, IT ease of management and compliance tracking. He explained that by "user-centric end-point IAM," he means a solution that balances the enterprise and IT requirements for monitoring, control and compliance with the end-user imperative of convenience.

It's this last element, user-convenience, which often gets left out of the equation as far as I can tell. And it could be a big reason why many IAM projects fail - or at least are less successful than predicted. d'Alençon explained why:

"The end-user is often left out of the equation when considering identity management solutions. The net result of the end-user omission is onerous: multiple tokens and badges that need to be persistently carried, different end-user experience and process for accessing different applications. This is costly both in terms of provisioning the various hardware for the system, in terms of time wasted by the end-user, and in lack of compliance when end-users try to 'end run' inconvenient processes and systems. Having end-users who WANT to use the system is certainly a more desirable situation. The solution must balance security with convenience. "

That's not an easy think to do, and requires a deft touch. But if you take the time to make it convenient for the user while maintaining the security you need then you can be very sure that you will have a successful project on your hands.

All contents copyright 1995-2006 Network World, Inc. <http://www.networkworld.com>