



## The Digital ID World Newsletter - March 30, 2006 Issue

By: Phil Becker ([phil@digitalidworld.com](mailto:phil@digitalidworld.com))  
Topic: General  
Posted: Thursday, March 30 @ 00:00:00  
URL: <http://www.digitalidworld.com/article.php?id=334>

Provided by Digital ID World, LLC.

FORWARDING THIS NEWSLETTER TO YOUR COLLEAGUES IS ENCOURAGED. If they would like their own subscription, send them to the Digital ID World web site to sign up at: <http://www.digitalidworld.com>

### In this Issue:

- The Network Perspective
- Digital Identity News
  - Security of Medicare info questioned
  - Two new Web sites let users find and report phishing
  - The hidden challenges of federated identity
  - nCipher Announces Release of Provisor 5.3 Update

==\*\*==

### Digital ID World Conference 2006

**\*Real-World Deployments\* \*Practical Advice\* \*Impactful Trends\***

Are you looking for real answers to tactical identity initiatives, planning and building a business case for your identity project, or trying to understand how future trends play into today's architectural decisions? Then Digital ID World Conference 2006 is for you.

Digital ID World is the only identity conference focused on putting end-users on stage, and only this focus brings you the conversations and answers you need to succeed. If your identity initiatives are focused on compliance, strong authentication, security, access control, provisioning, federation, rights management, or identity management - then Digital ID World is the one-stop you need to make.

Digital ID World Conference 2006

September 11-13, 2006, Santa Clara, CA

Register Now and Save!!



This is a classic example of a manual identity system. As I have often said, everyone has an identity management system - the question is only how much of it is manual and how much of it is documented. When you see teams of highly trained personnel sitting at tables with printouts manually correlating data to find out what they really wanted to know, you are looking at the modern equivalent of the 1950's room full of calculators - people with adding machines who did a company's calculating tasks. This is a situation begging for computers to automate it and return these talented peoples' energy to more productive tasks.

In the past several months, companies and products are starting to appear that are focusing on this part of the identity problem set. Two that come to mind are [A10 Networks](#) and [Identity Engines](#). While each of these companies sees the network/identity problem from a slightly different starting point, they have both designed identity appliances that bridge this network level gap that until recently has not been recognized as being part of the identity management realm.

These appliances are focused on solving the problems of integrating enterprise identity resources such as Active Directory or LDAP interfaced identity stores with the world of network devices that use Radius authentication or are part of the Cisco focused NAC consortium authentication universe. This universe has had many problems in scaling in any economical way, and integration with other identity sources has previously been largely unconsidered. By combining identity virtualization technology with a variety of identity management technologies these appliances are creating a bridge between the network itself and the higher level identity layers enterprises have been constructing for several years.

ROI is rapid with these devices, but what I find most interesting is the way that their existence impacts the outlook of those who have only seen the network from a deeply technical vantage point. When those people see some simple result of the integration of identity with their technical world, it is an immediate mind expanding experience. Simply seeing the identity of a user integrated into their security log reports, for example, opens their eyes to what network security is really all about - identity. Hours of work disappear, and a world of new possibilities opens up.

We are early in the development and deployment of this type of identity appliance (both of the companies mentioned only began shipping last Fall), but already it is clear that this is the next area of identity technology to reveal the power of integrating identity into the world view of those involved.

"Only when a person has constructed a conceptual framework do the facts begin to acquire meaning." And for most people it takes personal experience of some change in \*their\* world for that conceptual framework to really take shape. This is why the identity conversation is expanding on so many fronts right now, as identity suddenly spreads to many new areas where it will affect far more peoples' interests directly.

Identity was first seen (incorrectly) as security. Now that security is being seen to derive from identity things are coming full circle. The impact will be much larger than most suspect.

=====  
**Digital Identity News**  
=====

[Security of Medicare info questioned](#)

I bring you this USA Today article as a way of noting that once Electronic Health Records reach a certain momentum, we can expect to begin seeing this type of article a lot. If identity isn't well integrated with electronic health records (and today it's pretty spotty) then we can expect to see health identity data spills.

And if that starts to happen, the reaction will make the one we've seen to phishing look like nothing.

-----

## Two new Web sites let users find and report phishing

Speaking of Phishing, this article illustrates that we haven't made much \*real\* progress on it either. Since the failure of the Sender-ID effort, attempts at finding an internet scale email identity technology have slowed to a crawl. Without identity we are left with no good options. The one we gravitate to is one of the "Top 10 stupid security tricks" - listing the bad. Since there will always be more bad things tomorrow, "listing the bad" is a doomed effort.

Thus the larger the efforts to "list the bad" the more obvious it is that we don't really know how to fix the problem in any general way. Without identity we are stuck.

---

## The hidden challenges of federated identity

Federated identity may be the hottest arena in enterprise identity management today. But we are still on the frontier with it, and most deployments run into issues that the technology is the small part of.

This article by Phil Windley (Whose O'Reilly book titled "Digital Identity" is a terrific overview of the field) has written this article which gives good insight into the current state of federated identity, as well as what the real issues are that must be considered and how they need to be approached for success.

---

## nCipher delivers enhanced Provisor identity management solution

Last Fall nCipher acquired Chicago based Abridean, maker of the Provisor provisioning system. Now they have announced the first update of that software since the acquisition - Provisor 5.3. Provisor had already been focused on rapid deployment and ROI, but nCipher claims that this release broadens the arena where that is now true.

What is likely more significant, however, is the addition of tools that are focused on compliance, something no provisioning software can long prosper without.

The Identity Conversation continues...

Phil Becker  
Editor, Digital ID World

---

Please send your comments and feedback regarding this issue of the Digital ID World newsletter to:  
[editor@digitalidworld.com](mailto:editor@digitalidworld.com)

Copyright 2006 by Digital ID World, LLC  
P.O. Box 8777, CO 80201  
All Rights Reserved  
Permission to pass around freely granted

This article comes from Digital Identity World: <http://www.digitalidworld.com>