# Unified Identity Management


## Tom Olzak
## February 2006


Microsoft's new Windows project, code named Longhorn, is supposed to bring many improvements to the enterprise. Not the least of which is better overall security. But possibly the most interesting development is Microsoft's recent announcement about changes to Active Directory. These changes not only impact how user authentication and authorization are handled in your network. They also impact how you protect yourself on the Internet through the use of what Microsoft calls the Identity Metasystem.

In this paper, I explore the common identity and privacy challenges facing Internet users are they move from one content location to another. I'll then describe the thinking that led Microsoft down the path leading to its approach to unified identity management for the Internet – our final topic.

## The Challenges

Identity management on the Internet today is chaotic. There are two basic reasons for this. First, content providers and content users continue to use identity management tools and techniques that worked well on hard-wired networks. But the Internet, a global virtual network, doesn't lend itself to traditional approaches. Internet user identity activities are context-based. In other words, the identity information needed by each content provider depends on the perceived needs of the provider and the kinds of services or content delivered. This leads to the second reason – a lack of uniformity in how content providers implement identity management. Since approaches to identity management are based on requirements as viewed by each individual content provider, the internet is becoming a chaotic, unmanageable, insecure computing environment. Figure 1 depicts identity management on the Internet today.

Each content provider that requires information about the incoming user collects data and stores it for future use. User IDs and passwords might be different as the user moves from site to site. Because users have been trained to provide their information whenever an apparent content provider requests it, phishing and pharming attacks often successfully encourage users to provide personal information to Internet criminals. Short of criminal activity, content providers might also distribute personal information without the owner's knowledge or consent.

To summarize the current state of the Internet (Cameron, 2005),

1. There's no way to know who and what you're connecting to
2. There's no way to evaluate the authenticity of sites visited
3. There's no way of knowing when information is disclosed to illegitimate partners

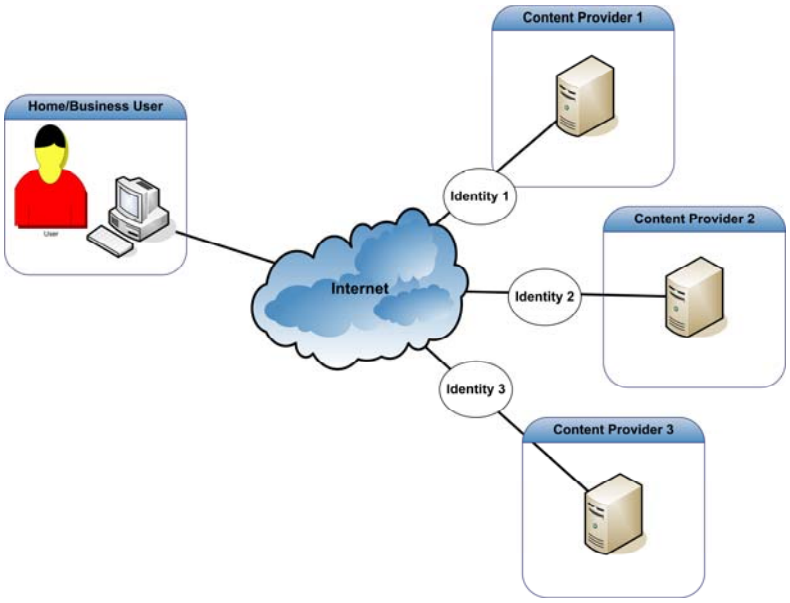


**Figure 1: Identity Management Today**

4.

# Conceptual Solution

*The Seven Laws of Identity*

Kim Cameron, Identity and Access Architect at Microsoft, described what is apparently the foundation for Microsoft's conceptual solution to the Internet identity challenges. In his paper, "The Laws of Identity," Cameron laid out seven Laws of Identity (2005). Before getting to the seven laws, it's important to understand some terms. The terms and definitions in Table 1 are from Cameron's paper.

**Table 1: Identity Terminology**

| Term | Definition |
|---|---|
| Identity Metasystem | "An interoperable architecture that assumes people will have several digital identities based on underlying technologies, implementations, and providers" |
| Digital Identity | "A set of claims made by one digital subject about itself or another digital subject" |
| Digital Subject | "A person or thing represented or existing in the digital realm which is being described or dealt with." (i.e. computers, digital resources, humans, and relationships between digital subjects) |

Cameron's list of the seven Laws of Identity:

1. Technical identity systems must only reveal information identifying a user with the user's consent.

2. The solution that discloses the least amount of identifying information and best limits its use is the most stable long term solution.
3. Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.
4. A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.
5. A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.
6. The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.
7. The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

To summarize the laws, digital identity is based on context. Because of the number of content providers, there are thousands of contextual variations. A solution is required that allows users to traverse these variations with a simple identity system within which they maintain complete control of their personal information. They must also have adequate assurance that they are not victims of online criminal activities.

*The Identity Metasystem*

Using the Laws of Identity, Microsoft developed the concept of the Identity Metasystem (Microsoft Corporation, 2005). The intended outcome of the deployment of a unified identity metasystem is a standardized approach to managing access, identity confirmation, and safeguarding user information on the Internet. According to Microsoft, the features of a metasystem include:

1. **Flexibility**. Personal information is not stored in the metasystem itself. This allows identity providers to decide where and how to store personal information.
2. **Open architecture**. The architecture is based on industry standard web services. This allows all identity providers to coexist with one another with equal status.
3. **User control.** Users have control over who gets their personal information.

This new approach to Internet identity management is rather aggressive. It requires a new underlying security infrastructure. So how does Microsoft plan to introduce the required features to its customers?

# Microsoft's Approach

Microsoft's Longhorn release includes a "new" Active Directory. No, it's not a complete replacement for the Active Directory (AD) we've all come to know and love. But it is an Active Directory that provides additional functionality focused on identity management. According to a Microsoft Product Information document (Microsoft Corporation, 2006), the Longhorn implementation of AD includes the following:

- Domain and directory services
- Strong credentials
- Access Control
- Single sign-on
- Federated identity
- Information rights protection
- Process automation
- Auditing
- Support for the issuance and management of "InfoCards"

For the purposes of this paper, we'll focus on the last feature in the list. The use of InfoCards is a big part of Microsoft's efforts to bring their products inline with what it sees as the conceptual solution to Internet Identity challenges.

*InfoCards*

The issuance and management of InfoCards is a key part of Microsoft's Identity Metasystem. Integrated into IE 7, InfoCard functionality targets online identity verification to reduce fraud and ID theft.

An InfoCard is a container or selector for a person's identities (Microsoft Q&A, 2006). Figure 2 is a simplistic example of how InfoCard technology works.

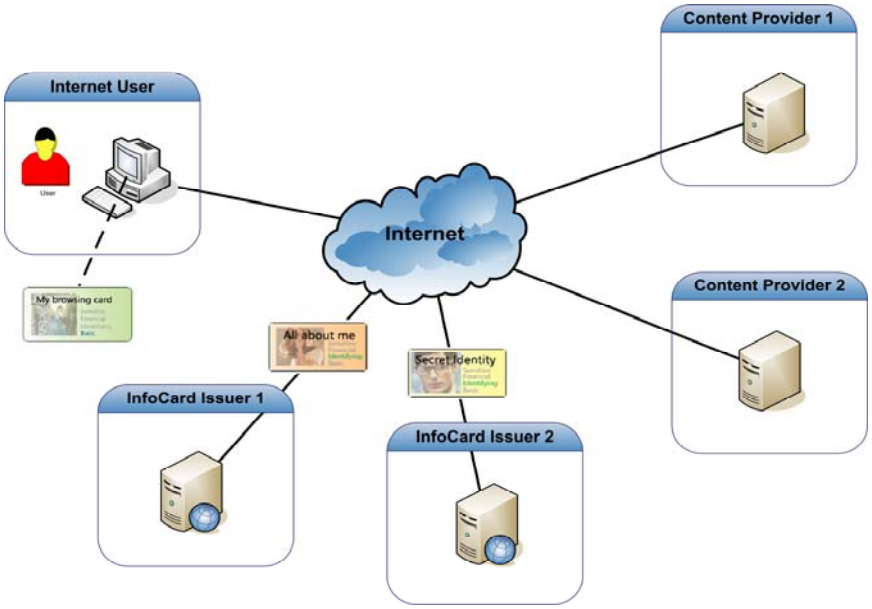


**Figure 2: Using InfoCards**

InfoCards can be issued by trusted vendors with which an Internet user develops a relationship or by the user. Each card is graphically represented on the user's desktop like an ID card. When the time comes to identify herself to a content provider, the user selects the most suitable InfoCard. Figure 3 is an example of how the InfoCard selection screen might look.

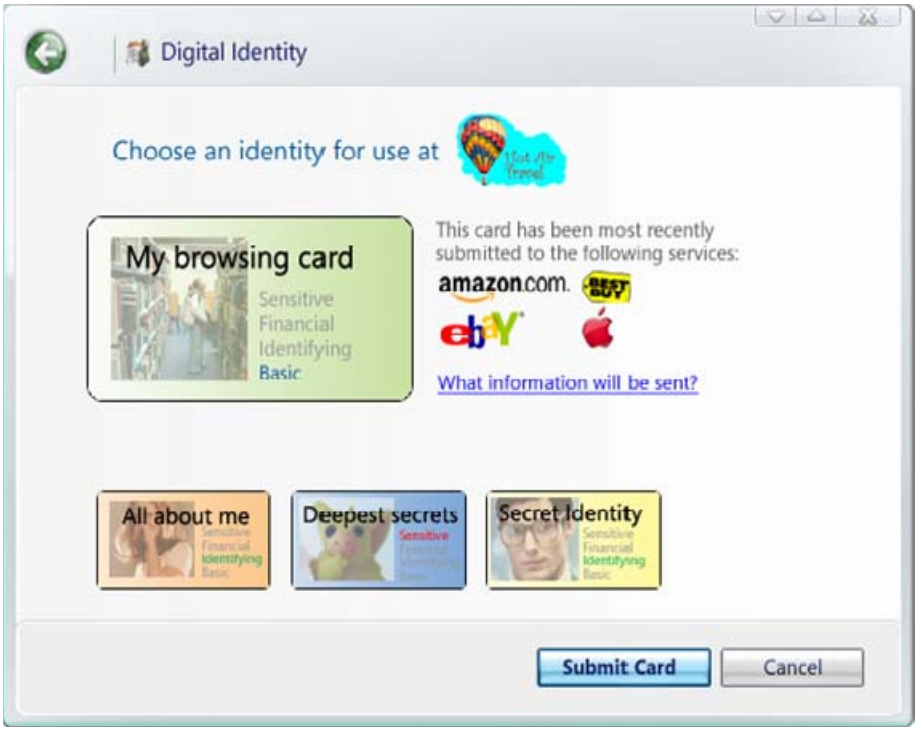


**Figure 3: Sample InfoCard User Management Screen**
(Fishenden, 2005)

From this screen, the user selects the InfoCard that provides the minimum information necessary for the current transaction, but no more. Once the content provider requesting the information is identified and verified, the InfoCard information is gathered from the issuing vendor's InfoCard information repository and sent to the provider. InfoCards also carry with them rules about how the information can be used. Finally, the user can review the content providers that have her various personal information sets based on the InfoCard used.

Using InfoCards to facilitate an identity metasystem looks like a good idea. Most, if not all, of the Laws of Identity are satisfied. Further, users interface with a standard identification process as they traverse the innumerable sites available on the global network. The perfect solution… well, maybe.

*Potential InfoCard Challenges*

There is still one important issue with which I'm still having trouble – InfoCard management. I think it's great that we're beginning to understand the special security and privacy needs of Internet use. But we must be careful we don't rush into a solution that might create bigger challenges than those we're trying to solve. Two of these challenges include:

- Each user becomes his own identity manager. Will the effectiveness of the identity metasystem require better awareness on the part of Internet users? If so, how will vendors provide that awareness? What processes will be in place to assist users in "cleaning up" problems they unintentionally create for themselves?
- InfoCards, and associated tracking information, are stored on the user's PC. What happens if the PC fails?

## Conclusion

Conceptually, an identity metasystem is a great solution for Internet identity management. With the cooperation of all vendors and content providers, users will possess a better way to manage and control their information and how it's used in Internet relationships. But will everyone accept this approach? Will enough Internet participants buy in to Microsoft's vision to make a difference? Will we deploy this new solution in a way that is palatable to the average Internet user? However we answer these questions today, tomorrow must provide a well-designed solution to Internet security and privacy concerns. Failure to work together to secure the growing global network could easily result in a future where people are afraid to engage in online commerce.

---

 Tom Olzak, MBA, CISSP, MCSE, is President and CEO of Erudio Security, LLC. He can be reached at tom.olzak@erudiosecurity.com or by visiting http://adventuresinsecurity.com

---

Works Cited

Cameron, K. (2005, May). *The laws of identity*. Retrieved February 22, 2006 from http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebsrv/html/lawsofidentity.asp

Fishenden, J. (2005, June). *Jerry Fishenden's weblog archives - June 2005.* Retrieved February 23, 2006 from http://ntouk.com/archives/2005/Jun/June%202005.htm

Microsoft Corporation (2005, May). *Microsoft's vision for an identity metasystem*. Retrieved February 22, 2006 from http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebsrv/html/lawsofidentity.asp

Microsoft Corporation (2006, February). *Microsoft announces vision and roadmap for Active Directory.* Retrieved February 22, 2006 from http://www.microsoft.com/windowsserver2003/evaluation/news/bulletins/ADvision.mspx

Microsoft Q & A (2006, February). *Q&A: advancing identity security on the Internet with "InfoCard" technology.* Retrieved February 22, 2006 from http://www.microsoft.com/presspass/features/2006/feb06/02-14InfoCards.mspx