



Suite 1, 85-87 Charles St Kew 3101  
PO Box 462 Kew, 3101  
Victoria, Australia  
Tel: +61-3-9851-8600  
Fax: +61-3-9851-8601  
[www.eb2bcom.com](http://www.eb2bcom.com)

Thursday 10 April 2008

## PRESS RELEASE

### Converging Metadirectory and Virtual Directory

Phil Hunt, now at Oracle, is the visionary responsible for a lot of the innovation in Virtual Directory. From his recent response to my ideas on second generation metadirectory, it looks like we are actually thinking about things in similar ways, where meta and virtual work together.

As you may know, there has been an ongoing discussion on what does the next generation of meta-directory look like. Kim Cameron's latest post elaborates on what he thinks is needed for the next generation of "metadirectory".

By "next generation application" I mean applications based on web service protocols. Our directories need to integrate completely into the web services fabric, and application developers must be able to interact with them without knowing LDAP.

Developers and users need places they can go to query for "core attributes". They must be able to use those attributes to "locate" object metadata. Having done so, applications need to be able to understand what the known information content of the object is, and how they can reach it. Applications need to be able to register the information fields they can serve up.

These are actually some of the key reasons I have been advocating for a new approach to developing identity services APIs for developers. We are actually very close in our thinking. Here are my thoughts:

There should be a new generation of APIs that de-couple developers from dependence on particular vendor implementations, protocols, and potentially even data schemas when it comes to accessing identity information. Applications should be able to define their requirements for data and simply let the infrastructure deal with how to deliver it.

Instead of thinking of core attributes as those attributes that are used in common (e.g. such as surname is likely the same everywhere). I would like to propose we alter the definition slightly in terms of "authoritativeness". Application developers should think about what data is core to their application. What data is the application authoritative for?

If an application isn't authoritative over an attribute, it probably shouldn't be storing or managing that attribute. Instead, this "non-core"

attribute should be obtained from the “identity network” (or metaverse as Kim calls it). An application’s “core” data should only be the data for which the application is authoritative. In that sense, I guess I may be saying the opposite of Kim. But the idea is the same, an application should have a sense of what is core and not core.

Applications need to register the identity data they consume, use, and update. Additionally, applications need to register the transactions they intend to perform with that data. This enables identity services to be built around an application that can be performant to the application’s requirements.

What I have just described was actually part of the original inspiration behind CARML (Client Attributes Requirements Markup Language) put forward by Oracle that the Liberty Alliance is working on now. It was our belief that in order to enable applications to connect to diverse identity service infrastructures, something like CARML was needed to make the identity network both possible, adaptive, and intelligent.

But, while CARML was cool in itself, the business benefit to CARML was that knowing how an application consumes and uses identity data would not only help the identity network but it would also greatly improve the ability of auditors to perform privacy impact assessments.

We’ve recently begun an open source project at OpenLiberty called the IGF Attribute Services API that does exactly what Kim is talking about (by the way, I’m looking for nominations for a cool project name - let me know your thoughts). The Attribute Services API is still in early development stages - we are only at milestone 0.3. But that said, now is a great time for broader input. I think we are beginning to show that a fully de-coupled API that meets the requirements above is possible and dramatically easier to use and yet at the same time, much more privacy centric in its approach.

The key to all of this is to get as many applications as possible in the future to support CARML as a standard form of declaration. CARML makes it possible for identity infrastructure product vendors and service providers to build the identity network or next generation of metadirectory as described by Kim.

I haven’t seen CARML - perhaps it is still a private proposal? [UPDATE:

I’ve been advised that CARML and the IGF Attribute Services API are the same thing.] I think having a richer common representation for people will be the most important ingredient for success. I’m a little bit skeptical about confining developers to a single API - is this likely to fly in a world where people want to innovate? But details aside, it sounds like

CARML will be a helpful input to an important industry discussion. Above

all, this needs to be a wide-ranging and inclusive discussion, where we take lots of input. To get “as many applications as possible” involved we need to win the participation and support of application developers - this is not just an “infrastructure’ problem.

Oberursel and San Francisco, Sept. 19, 2007 / Utimaco – The Data Security Company, today announced at the Intel Developer Forum support for the next generation of Intel® vPro™ processor technology, be made available in the second half of 2008. Under the cooperation, Utimaco SafeGuard® solutions will provide key and policy management for Intel’s hardware-based encryption technology, codenamed Danbury technology. Utimaco plans to integrate Danbury capabilities with SafeGuard data security functionalities, for enterprise-wide management of data encryption.

"With the integration of Intel’s chipset-based technology under our management platform SafeGuard Enterprise, customers get the best of both worlds: Hardware-enabled encryption with enterprise-grade data

security management,” said Malte Pollmann, Executive Vice President Products, Utimaco. “Working together, Utimaco and Intel are combating the dangers of unprotected data on mobile and desktop PCs.”

- end -

eB2Bcom is a reseller of Identity Management products please contact us on :

**eB2Bcom**

Tel: 03 9851 8600

Fax: 03 9851 8601

Web: <http://www.eb2bcom.com> , <http://www.view500.com/>