DANCING AROUND IDENTITY

(No. 1 of the Identity Planet series)

by

Timothy Grayson

ABSTRACT:

Networked computing is the most pervasive and significant information technology development of the recent past. As the protective walls of computer and data isolation have come down, location-based identification methods have become inadequate. Location-independent, strong "digital identity" is required to move ahead with the development velocity to which we've become accustomed. But as we race ahead trying to find a solution or solutions, crucial questions remain unanswered and, in some cases, even unasked. In this paper, after a brief description of the subject's topography, we ask these questions in preparation for the remainder of the Identity Planet *series of papers, which attempt to address the questions in some depth. The risk of not having lengthy discussions around these questions is the very real potential for a series of* ad hoc, *near-focus initiatives that will pollute the environment for the longer term.*

DANCING AROUND IDENTITY

by

Timothy Grayson

The most pervasive and significant information technology development of the recent past is networked computing, brought into greatest relief by the Internet. As the protective walls of computer and data isolation have tumbled under the weight of need and desire to expose information, location-based user and equipment identification has become inadequate. That realization has cast a strong light on finding a location independent, strong, reliable, and robust means of properly and certainly identifying entities – particularly in cyberspace.

The solution is "digital identity," the essence of which is identifying physical entities in the virtual world by assigning each a unique digital identifier. Digital identity exists for objects attached to a network, but, while important, we are concerned with the identity of people that are attached to the network from time to time. Digital identity is not by itself, however, a solution. It is an encompassing notion – inclusive of a number of solutions to specific problems – for the foundation of a new paradigm in networked computing. The novelty of this notion that sets it apart form the ideas of identity (pin/password, etc.) that have existed for years is that it refers to *strong* identity now. Strong identity being rigorously authenticated and of high systemic integrity.

A primary driver for strong digital identity is Web services. These distributed computing applications perform valuable activities through machine-to-machine requests for access to or use of proprietary data/applications. The Web services and distributed computing approach presumes a fundamental shift from a location-dependent, perimeter security paradigm to a location-independent approach. It is the modern, digital equivalent of the historic eclipse of ramparts and city walls by a national security dependent on distribution and mobilization of ready strength. This, of course, demands strong identification of not only the machines that are talking to one another, but of the humans for whom those machines are working and their rights to the data/applications.

While a broad swath of activity can be addressed by digital identity solutions, because of the early days in this field, to move ahead we must bound the contemplated space. Strong digital credentials can be used offline to augment more traditional means of identification such as visual proof, magnetic stripe cards, and so forth. While peripherally referring to such uses, including national identity cards and digitally encoded driver's licenses, a more fundamental concern must be establishing high-integrity digital identities for online activity where there is no physical manifestation – or opportunity for secondary visual validation – of the identified entity. The requirements of the online environment are more demanding than all others and therefore becomes the minimum acceptable capability set.

Security and privacy concerns have, particularly since the last quarter of 2001, commanded significant energy and concern. Everywhere, traditional approaches to heightening security are being augmented with digital credentialing. Strong credentials and bio-based solutions for finite closed populations are in the fore. They are expensive and limited by/to the closed environments they serve. Such tools have long been employed in facilities where the need for security has warranted their expense such as police or government installations and R&D labs. Most organizations have not until now, however, found a financial reason to implement such structures. Nor have they, until now required digital identity to address open environments (say, customer-directed Web services) in addition to the typical closed loops of employees and established business partners.

Focus on physical security should not suggest that logical access for online network activity has been overlooked. Physical security is merely more visible and easily understood. Logical access solutions are being sought aggressively to combat increasing online crime and nuisance activity. But many organizations still do not fully appreciate that the perimeter-guarding methodology is inadequate for the demands of the evolving online world. Consequently, as a result of secondary focus and outdated approaches, the shift to more robust digital credentialing continues to trail behind. Fortunately, however, the same digital credential technologies that are being evaluated and considered for the physical processes can be used for logical accesses as well, which has accelerated the implementation of *common access card* (CAC) systems in many organizations.

Privacy is a key cause for stronger digital credentials. Concerns here result from awareness of the extensive pools of information and data about individuals that have collected in the nooks and crannies of the wired world. The velocity and ease with which disparate stores of data can be aggregated, parsed, and re-organized to create bodies of knowledge about individuals is – or at least ought to be – a concern to everyone. What privacy is and whether it even exists, however, is contentious. Moreover, it is culturally and contextually dependent. In this context, “privacy” generally refers to the ability to control the dissemination of information about us that we believe can be used to invade our personal space (whatever that might be). We want to discretely constrain information distribution from others – to have privacy –in fluid circles of proximity and need. Whether there is even any right to do so, stemming from uncertainty about what information about ourselves we *own* and can therefore control, is questionable.

Regardless of the ownership issue, only by proper management of authorization and access to information through strong digital credential can these bits of data be kept from prying electronic eyes. Theoretically this may be a good approach because it puts the discretion to disseminate and use information on a by-use basis into the hands of the information’s owner. In the details, of course, are many definitional and logical shortcomings that stall the concepts short of a practical solution, not the least of which is the ownership issue.

Some argue that the digital identity cure is worse than the disease – or fear of disease, actually – that engenders it. Among other things, the creation of digital identities also creates new treasure troves of valuable, aggregated data. And, it eliminates all but a single key to the vault, making the reward for breaching the identity data store more valuable. The underlying premise upon which these lines of thought are built, however – that of a single identity equaling a single authoritative credential – may not be valid. It is, at the moment, a subject of heated debate.

Compelling evidence mounts from both the supply (e.g., ready and available technology) and the demand (e.g., CAC ID cards, trusted traveler cards, etc.) sides that digital identity is on the rise. But crucial questions remain unanswered and, in some cases, unasked. At both the philosophical and practical levels, some conclusion is required. Questions about the digital identity *of people* to stimulate thinking might include:

- What is a digital identity and is it the same as a digital credential? Can multiple identities exist for the same entity? Is a digital identity different than the physical identity? How do *roles* or *personas* fit into the picture?
- Supply and demand have been primarily contemplated within closed environment settings. Although recent attention has been migrating toward general use digital credentials, implementation and evolution models remain founded on closed environment premises. Is this the correct approach? Can closed system solutions, federated together, provide a rigorous, high-integrity open system solution?
- Have we considered the means for fail-safe distribution of credibility, trust, etc., in a scaled and scaleable manner that is fully inclusive and can accommodate development?
- Without the imposition of a single, (perhaps) state-enforced standard for digital credentials, how will the forces of competition address the issues of trust, credibility, and interoperability? Who will accept the liability for standing up on behalf of a digital identity assertion in an open environment?
- Can any comprehensive, high-integrity system exist without a regulated and (state-) enforced initial authentication system?
- Given that the costs of large-scale solutions are extraordinary – particularly for pioneers – and that many are too costly to use given the limited benefit afforded to many users, how might the market evolve? Who will sustain those investments? Why?
- What are likely solutions, how many are likely to persist and prevail, and how will they interoperate?
- Federation of identities is an interesting concept that satisfies certain needs, primarily those of convenience and CRM. Does it reflect social reality and adequately offset frictionless convenience and transparency with the desire for personal privacy and the opacity of information stored?

These are not novel queries, as many people involved in this exploding field have posed them before. They do require address and debate. The risk of not contemplating them – even the more tedious philosophical questions that trouble business people – is the very real potential for a series of ad hoc, near-focus initiatives being deployed only to pollute the environment for the longer term.

In this series of essays, entitled *Identity Planet*, I dance around these questions to provide some perspective to the novice and – hopefully – jump-point ideas for the structuring of a long-term evolutionary solution.

XXX