



Have Identities Before You Manage Them

The need to establish identity prior to identity management system construction

March 2007

Table of Contents

Introduction.....	3
“The Internet Is Broken.”.....	3
What's the damage?.....	3
Identity, the support beam of Information Architecture.....	3
Retiring old assumptions.....	3
If it's broke, fix it.....	4
Building a better architecture.....	4
Buildings.....	4
Quiet Enjoyment.....	4
Virtual Reality.....	4
The need for reliable identities.....	5
Constructing Identity.....	5
The guiding principles of IMA.....	5
IDQA™.....	5
Levels of Security.....	5
The Six Dimensions of IDQA™.....	5
Conclusions.....	5

© 2007 Authentrus, Inc. and/or Its Affiliates. All Rights Reserved. Authentrus, IDQA, Six Dimensions of IDQA and Authentrus Law of Security are trademarks or registered trademarks of Authentrus, Inc. in the US and other countries. This document shall not be duplicated or used for any purposes other than those for which it is being provided. The information contained herein was originated by and is the property of Authentrus and except by rights expressly granted by written consent, such information shall not be disclosed or disseminated in whole or in part. Authentrus reserves all patent, proprietary, design, use, sale, manufacturing and reproduction rights hereto. The information contained herein has been obtained from sources believed to be reliable. Authentrus disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Authentrus's research may discuss legal issues related to the information technology business, Authentrus does not provide legal advice or services and its research should not be construed or used as such. Authentrus shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.

Introduction

All networks, including enterprise networks, are afflicted by the same fundamental problem: inauthenticity.

Because more and more of what we do takes place through our digital window on the world, inauthenticity anywhere affects reliability, manageability, and security everywhere.

This paper focuses on the quality of identity infrastructures, and the resultant impact on reliability, security, manageability, and authenticity.

“The Internet Is Broken.”

So reads the cover story of MIT's *Technology Review*,¹ summing up in few words the troubled state of our public information infrastructure, once aptly known as the 'Information Highway.'

In the article, MIT's David D. Clark, the National Research Council's Computer Science and Telecommunications Board chairman says, “The Net's basic flaws cost firms billions, impede innovation, and threaten national security. It's time for a clean-slate approach.”

For business consumers, a clean-slate approach is imperative.

What's the damage?

On the Internet, the questions raised by a lack of authenticity are: can I trust this offer, this link, this site?

In the corporate network, the questions are: who has access to that file / the data for this week's analyst conference call / the plan details for the new product rollout?

Security and manageability have become more elusive as available technology has become more powerful. If we consider what Identity Management is intended to fix, it is apparent that the Internet isn't the only thing that's broken. Whole corporate networks are broken.

Telecommuters have made home computers (even those protected by VPN and NAC technology) part of corporate networks. Inauthenticity in the system causes problems beyond anonymous adult predators purporting to be a child's peers in social networks such as MySpace.

Spyware in home machines allows anonymous criminals operating from untraceable remote outposts the ability to steal more than bank account usernames and passwords. Even organizations that have completely isolated their networks from access by home computers and mobile devices suffer problems caused by online inauthenticity.

Identity, the support beam of Information Architecture

The prime corporate information infrastructure to service this broken Internet is the identity infrastructure.

Identity Management, the business of applying identity records in an information infrastructure, is a fairly well developed discipline.

As described in the literature of Identity Management, its various parts may be grouped into two categories:

1. **Provisioning of Identities**
2. **Application of provisioned identities to online resources**

Identity Management (IDM) is often deployed by companies for reasons that have more to do with efficiency and economy than security. Allowing new employees to be productive right away by provisioning information resources quickly can justify the entire investment in licensing and deployment of IDM software. The productivity-related reasons for adopting Identity Management can tend to obscure the fact that reliable management of identities introduces possibilities for whole new levels of security and manageability with new sources of cost reduction.

Retiring old assumptions

Before the identity revolution began, information security was all about packet filtering, which when packaged into an appliance become known as a “firewall” / “intrusion detection system” / “intrusion prevention system” / “unified threat management appliance,” etc. Packet filtering is residue from the days when the Internet was viewed as the new frontier, inhabited by open-range cowboys whose understanding of security was that every packet came from either a good guy or a bad guy. The job of the security appliance was to drive the bad packets away from the encampment.

In the physical world, when agendas became complicated beyond cattle drives, cities developed. The relevant assumptions behind identity management in the modern world are more like the existing assumptions of an office building than those of an outpost. Identity management, where the identities are established through reliable means, is the first step toward making information infrastructures infinitely more manageable and secure.

In the current IDM framework, provisioning is identified as the beginning of the Identity Management process. Provisioning is, in short, the filling in of application usernames and passwords by the identity management system, so that it may act as a proxy for future uses. The fundamental assumptions of provisioning are:

1. **Available identities are sufficiently reliable for all purposes**
2. **An identity is a manifestation of relationship**
3. **Identity credentials are not shared**
4. **Identity Management starts with provisioning**

Let's evaluate those assumptions.

Available identities are sufficiently reliable for all purposes

This might be a safe assumption, in the case of the single office of a very small, well-established firm consisting only of long-term employees, working in one location. As we consider larger organizations, where contractors and freelancers and consultants and ad agency personnel and outside lawyers and suppliers connect from multiple locations, the notion of reliable identities begins to elude us. This happens long before we start to consider federated identities and circles of trust.

An identity is a manifestation of relationship

Relationships change. People get transferred, promoted, assigned from newly acquired subsidiaries, go from full-time to part-time and vice versa. As long as we have a staff function that is dedicated to keeping identity records up to date, relationship-based credentials are workable.

After all, network access credentials aren't like drivers' licenses or passports, which are based upon the permanent, immutable, relationship-free credential known as a birth certificate. Is this because drivers' licenses and passports

¹Talbot, David, December 19, 2005. “The Internet Is Broken”, *Technology Review*, Dec/Jan '06.

are more important? Does this mean that relationship-based credentials should be used only to access unimportant network resources? That nothing of real significance should ever be done online?

We at Authentrus believe that the propensity of people to subvert the security of an information system is proportional to the value to be gained by doing so.²

As long as nothing important is going on in your network, you needn't worry about the reliability of the identity credentials relied upon nor the identities they represent. If you feel your network needs to grow in importance, then you should look at the quality of the identities underneath its access credentials.

Identity credentials are not shared

If a newly assigned project team member needs access to a file right away in order to meet a deadline, we can expect the sharing of credentials to occur in order for the deadline to be met. Usernames and passwords are routinely shared in such situations, despite policies with stern penalties for doing so. It's how work gets done. Speed of credential issuance in fact is one of the motivating factors in the adoption of Identity Management. Yet even when the issuance of typical relationship-based credentials is quick and efficient, usernames and passwords still get shared, typically when users and managers don't see eye to eye on what permissions are needed to perform a task.

Now, suppose the access credential were the employee's bank ATM card. What would happen if a new team member asked to borrow his colleague's card and PIN? He would never make such a preposterous request, of course. The uncomfortable truth is that a credential that protects your company's assets gets more casual protection than the one that protects the user's own assets. Therefore, a credential that has a degree of universality is inherently superior to a credential that only represents a single relationship, as between employer and employee.

Identity Management starts with provisioning

Because we are already unsure that our identities are reliable, provisioning is premature. A sound approach to Identity Management starts rather with an assessment of the degree of identity quality needed for each group of digital assets, and each group of users needing to access that group of assets. The next step is enrollment, or the establishment of identities with the requisite level of reliability.

The fundamental assumptions of provisioning do not hold up in the light of scrutiny.

If it's broke, fix it

How then do we develop our clean-slate approach to building identity infrastructures? Let's start with some new assumptions:

1. **A viable identity infrastructure starts with identity quality needs assessment, not provisioning.**
2. **Reliable Identity Management starts with reliable identities.**
3. **Reliable identities are the product of sound enrollment practices.**
4. **Credential sharing and other problems are mitigated when the user owns his or her own universal credential.**

To get to our reliable identity management system from here, we must first ask: Where did our identities come from? ³

What was the enrollment process? Who is liable for consequences of enrollment problems? The enrollment officer? The enrollee? Both? If we don't ask the question we are left with the answer that the organization that uses the identities is responsible for problems with them.

Building a better architecture

An equation for identity information architects to live by:

Identities + Identity Management System = Identity Infrastructure

This may appear to be a statement of the obvious, however the IDM discipline consistently ignores the process of establishing identities, and we find only cursory treatment of credential quality. Reliable identities are essential to a reliable identity infrastructure, and consequently to a reliable information infrastructure. Conversely, good management of unreliable identities is a waste of skills and money.

In his book *Digital Identity*, Phillip J. Windley provides a valuable metaphor for enterprise architecture:

"In the same way that city planning creates a set of standards and rules for buildings to ensure that neighborhoods are safe and pleasant, an enterprise architecture is a set of standards and rules that creates an interoperable and flexible enterprise-wide IT infrastructure. The work of city planners provides a model that helps us understand the work required of enterprise architects." ³

This metaphor is essential to understanding how to build strong identity information architectures.

Buildings

In order to build a strong identity information architecture, one must know how a building works. This is because office suites and meeting rooms and filing areas and personal workspaces and other spaces have boundaries, where groups of specific people can focus on their mission in order to get things done. Real estate lawyers call this "quiet enjoyment."

Quiet Enjoyment

Quiet enjoyment is a two word summary of the terms of a commercial lease. It is what a property owner owes a tenant in good standing. Quiet enjoyment means not just secure main doors but serviceable interior walls and clean working elevators, suitable common areas, and other useful amenities that distinguish an office building from a fenced-in area on the open plains.

Virtual Reality

Despite the remarkable similarities between well-designed physical facilities and online facilities, one big difference stands out. Visual and aural cues tell us who is in a physical room with us. Online, we have to rely upon identity records to tell us who is in what room, touching what files, engaging in which collaboration sessions.

Let's look again at the real estate metaphor from Phillip Windley's *Digital Identity*⁴:

"In the same way that city planning creates a set of standards and rules for buildings to ensure that neighborhoods are safe and pleasant, an enterprise architecture is a set of standards and rules that creates an interoperable and flexible enterprise-wide IT infrastructure."

When the benefits of Identity Management are discussed in

² Authentrus Law of Security™

³ Windley, Phillip. 2005. "An Architecture for Digital Identity" in *Digital Identity*. Sebastopol, CA: O'Reilly & Associates.

⁴ Ibid.

books, white papers and professional literature, the real estate view of facilities frequently is invoked, primarily because the metaphor has legs. As we drill down into the way buildings are designed, built, permitted and managed, we find that information facilities can be treated very much as though they were physical facilities. The major difference is that in an online building we have a sort of sensory deprivation. Instead of a mass of visual and aural cues that tell us who is in a particular room at a particular time, we must rely upon identity credentials to tell us.

The need for reliable identities

Identity Management therefore starts us on the path of being able to use building management ideas and methods with online facilities, an easier and more effective way to do it. But the real estate metaphor also highlights in this case the need for reliable identities.

Architects, structural engineers, contractors and building inspectors are personally licensed by duly constituted public authority. Reliable identities of those professionals appear on plans that are filed with the city and its planning department. If a building sags, drops roofing materials on passersby, or falls down, one or more of those individuals will be in jeopardy of losing their license – their authorization credential – to practice their profession. The fact that a personal asset – one's ability to earn a livelihood – is tied to the credential is what ensures that it will be protected by its holder.

With licensed real estate professionals, having identities is more important than managing them. An enterprise's need for identities would seem to be different, but there is a clear lesson from the architecture, engineering, and construction industries that is applicable to any enterprise. That is, identities that are owned by those identified are a source of accountability.

Constructing Identity

With identity as the support beam of information architecture, reliable identity would seem the obvious meter by which an Identity Management Architecture (IMA) is measured. Up until recently however, reliable identity was not an assumption in IMA construction.

The guiding principles of IMA

Chapter 13⁵ (**An Architecture for Digital Identity**) of Phillip Windley's book provides us with the guiding principles of IMA. We will refer to two of the most important here:

1. Identity management requires that resources and entities be identified first. Typical information security plans are largely about perimeter defenses. Consequently, they are usually concerned with networks and servers rather than business documents and customers. Like the functional business model, the level of detail in the inventory of resources and entities varies depending on the nature of the IMA planning process, but these are its central focus.

2. An IMA identifies dependencies between identity data and systems. These dependencies are used to determine implementation priorities. Security planning, and most IT planning for that matter, often emphasizes projects that are deemed critical without seriously considering dependencies between data and systems. An IMA highlights those dependencies so that they can be used in the planning process.

IDQA™

Identity Quality Assurance (IDQA™) is a methodology and

accompanying set of procedures (developed with Phillip Windley's guiding principles in mind) for assuring that an identity credential is appropriate, as measured in each of six categories, for the part systematic method for determining level of enrollment.

IDQA™, as an integrated set of components, is quite new, and includes measures to judge the effectiveness of, for example, the latest Bluetooth identity tokens. But some of the newness in fact represents a new application of concepts as old as those used by the Tabellione of ancient Rome.

Levels of Security

Different workgroups and applications have varying requirements for security, assurance of authenticity, and manageability. A judge responding via secure PDA to a police detective's request for a warrant will for example require a very thorough PKI based system with three-factor authentication and long cryptographic keys, while a warehouse data entry function may be just fine with usernames and passwords assigned as a function of a provisioning step. The different parameters include: degree of financial risk, characteristics and degree of non-financial risk, requirement for non-repudiation, duration of assignment, and many others.

The Six Dimensions of IDQA™

IDQA measures identity quality in six "dimensions":

- 1. Independence of credential from relationship**
- 2. Quality of Enrollment practices**
- 3. Quality of Certification**
- 4. Quality of the Credential**
- 5. Assumption of Liability**
- 6. Quality of Implementation and Management**

Consider changing your enterprise's role in the identity infrastructure, leaving the role of IDP (Identity Provider) to an outsourcer and becoming a PRP (Principal Relying Party). This will have the following effects:

- 1. Since users own their credentials, they are responsible for their own password resets. It then becomes their job, not yours, to maintain a working identity credential.**
- 2. End sharing of identity credentials**
- 3. End credential revocation problems at termination**
- 4. Have the benefit of clear liability assumption by the Identity Provider**

Conclusions

An IDQA™ assessment, combined with a change in roles from identity provider to principal relying party, will make your identity infrastructure more workable. In turn, your enterprise's whole information infrastructure will become more manageable, more economical, and more secure.

To bring the benefit of a reliable identity infrastructure to your enterprise, get in touch with Authentrus.



738 Main Street
Waltham, MA 02451

+1 781 647 7178
info@authentrus.com

5 Ibid.