

Logic Trends Inc. Identity Management Series

Identity Unification: A Logical Approach



Logic Trends, Inc.
www.logictrends.com

Atlanta

1050 Crown Pointe Parkway
Suite 295
Atlanta GA 30338
office: 770.551-5050
info@logictrends.com

Dallas

Tampa

Cleveland



Identity Management Solutions for Today's Business Trends

Identity Unification: A Logical Approach

White Paper

Abstract

A white paper from Logic Trends discussing the complex issues surrounding directory unification with Legacy and other non-directory environments. An audience with a cursory understanding of the simplified sign-on and eProvisioning problem space will adequately absorb and relate to the content of this paper. Specifically, this paper will discuss the cause, affect, and resolution of complexity surrounding the task of unifying disparate data sources into a single enterprise directory. Many of the concepts discussed in this paper also provide deeper insight into the meta-directory, provisioning, and Simplified Sign-on problem as a whole, benefiting strategic planners tackling this complex problem.

June 03, 2003
Version 3.0

©2004 Logic Trends, Inc. All rights reserved.
Written by Phil Lentz

To provide feedback on this white paper, please send e-mail to info@logictrends.com.

The information contained in this document represents the current view of Logic Trends on the issues discussed as of the date of publication. Because Logic Trends must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Logic Trends and Logic Trends cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. LOGIC TRENDS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Logic Trends, enFuse, enForm are registered trademarks of Logic Trends.

Other product or company names mentioned herein may be the trademarks of their respective owners.

Logic Trends • 1050 Crown Pointe Pkwy • Atlanta, GA 30338 • USA



Logic Trends, Inc.
www.logictrends.com

Atlanta

1050 Crown Pointe Parkway
Suite 295
Atlanta GA 30338
office: 770.551-5050
info@logictrends.com

Dallas

Tampa

Cleveland



Contents

INTRODUCTION.....	4
CURRENT SOLUTION DOMAINS	4
SIMPLIFIED SIGN-ON (SSO)	4
POLICY SERVICES.....	5
PROVISIONING	5
META/VIRTUAL DIRECTORY	5
SUMMARY	6
BUSINESS PROCESSES AND IDENTITY MANAGEMENT	6
IDENTITY BUSINESS PROCESSES	6
MULTIPLICITY	7
WHAT CAN TECHNOLOGY DO?	7
SUMMARY.....	8
IT'S ABOUT THE PEOPLE, NOT THE ENGINEERING!.....	8
HUMAN FACTORS	8
ACQUIESCENCE	9
ACCEPTANCE	9



Logic Trends, Inc.
www.logictrends.com

Atlanta

1050 Crown Pointe Parkway
Suite 295
Atlanta GA 30338
office: 770.551-5050
info@logictrends.com

Dallas

Tampa

Cleveland



Introduction

This paper will take a hard look at the challenges facing projects focused on one or more dimensions of Identity Management:

- 1) Simplified Sign-on
- 2) Policy Services
- 3) eProvisioning
- 4) Meta-Directory

Once the problem space is understood, we will explore how the problem domains are impacted by day to day operations and business processes. In closing, this paper will discuss a solution approach that addresses the reality of day to day operations.

Current Solution Domains

It is important to first understand the major identity related initiatives and compartmentalized product offerings featured in the industry today. This discussion will help us infer a deeper understanding of the resistance imposed by “real” business processes. This information, in turn, will provide a foundation for discussing a business focused Identity Management approach.

Simplified Sign-on (SSO)

Also known as single sign-on (SSO), this aspect of Identity Management has the following objectives:

- 1) **Single Set of Credentials** - A single, unified set of authentication credentials for accessing applications, operating systems, and databases
- 2) **One Time Authentication** - Providing access to multiple applications, operating systems, and databases based on a single authentication act which in turn provides admittance to more than one application

SSO project warriors know the duration of such a project can seem never ending. Consequently, a more realistic “simplified” sign-on approach is often taken first to provide one time authentication for custom web based applications. While a second, incremental (a.k.a. wait and see), strategy for third party and desktop applications is taken later. This one-two strategy provides time for third party application vendors (i.e. ERP, CRM, etc) and custom application developers to successfully integrate with LDAP based directory services. The reason web applications are often considered an easier target for SSO than “fat client” applications is the inherent web based session architecture provides a vehicle for sharing an authentication context across multiple applications.



Logic Trends, Inc.
www.logictrends.com

Atlanta

1050 Crown Pointe Parkway
Suite 295
Atlanta GA 30338
office: 770.551-5050
info@logictrends.com

Dallas

Tampa

Cleveland

Policy Services

Policy services represent a collection of APIs, plug-ins, and connectors focused on providing:

- 1) Authentication
- 2) Role and group based access control (authorization)
- 3) Password management
- 4) Fine grained access control (granular, code level, authorization)

Solutions in this category typically sit on top of an LDAP directory that stores user profiles, credentials, roles, and authorization resources (a.k.a. entitlements). Third party vendors often provide web server, application server, portal, and ERP plug-ins that automatically challenge the user for authentication and provide limited high level authorization to screens and web pages. However, fine grained access control is not provided by these plug-ins due to the intrusive (code level) nature of the problem. In addition to plug-ins, a robust set of APIs is typically offered to provide session based, fine grained access control (authorization) and user administration capabilities. Finally, a robust administration console is provided for internal and delegated administration capabilities.

Provisioning

Products and solutions in this category take the following approach. If you administer and provision user accounts from a single interface and push the authentication credentials and identity data to all identity data sources, you have provided federated identity management. These tools typically satisfy the following "Use Cases":

- 1) **New Requests** - Handle account change requests (create, modify, revoke, etc)
- 2) **Validation** – Insure account data is correct and complete
- 3) **Approval work flow** – Route change request to all concerned parties for approval
- 4) **Identity propagation** – Push change to multiple systems interested in identity data
- 5) **Notification** – Alert all concerned parties of the change

These features are focused on streamlining the user provisioning workflow and disseminating identity related data to support enterprise applications. Most products rely heavily on a directory to provide meta-data and staged account storage.

Meta/Virtual Directory

Products and solutions in this category take a data replication and unification approach. The focus is on creating a unified directory either real or virtual that synchronizes or "views" identity data sources containing user profile, credential,



Logic Trends, Inc.
www.logictrends.com

Atlanta

1050 Crown Pointe Parkway
Suite 295
Atlanta GA 30338
office: 770.551-5050
info@logictrends.com

Dallas

Tampa

Cleveland

group, role, and entitlement data. Each data source may publish or subscribe to changes from other data sources connected to a meta directory. Whereas, a virtual directory places an LDAP view on existing sources and is less concerned with synchronization and more focused on routing LDAP requests to a variety of data sources:

- 1) Directory/LDAP
- 2) Legacy
- 3) Unix
- 4) Microsoft OS
- 5) Relational

Summary

Armed with a cursory understanding (or refresher) of current products and solutions that address the Identity Management space, you are now prepared to explore the union of business reality with technology in the Identity Management space.

Business Processes and Identity Management

After reviewing the many different Identity Management ingredients in the previous section, one begins to understand the complexity of the identity management problem space. Each part approaches the identity problem from a different angle (as a cog in a bigger machine). While each product vendor can tell you which specific technology and data issues are addressed, they may fear to share with you how to complete a unified SSO and Identity Management project on time and within budget. Though the ultimate goal is to provide unified identity management and simplified sign-on for the enterprise and extraprise¹, the harsh reality is that very few have ever succeeded. Maybe taking a closer look at the business process will shed some light...

Identity Business Processes

Let's take a moment to look at the human dimension of the identity management process within the business community. The following points represent the majority of identity related scenarios ("Use Cases") in a typical business case:

- 1) Administrators provision (create) new employee, partner, and customer accounts (henceforth, these will be termed Identity)
- 2) Employees, partners, and customers change passwords voluntarily or through a password expiration prompt
- 3) Administrators reset expired and forgotten passwords

¹ This term reflects enterprise capabilities that are offered to non-employee users. If this term is adopted by the community or has been contrived by someone else, I offer my sincere apologies


Logic Trends, Inc.
www.logictrends.com

Atlanta

1050 Crown Pointe Parkway
Suite 295
Atlanta GA 30338
office: 770.551-5050
info@logictrends.com

Dallas

Tampa

Cleveland

- 4) Administrators revoke identity credentials
- 5) Administrators set up entitlements for identities, roles, and groups
- 6) Users authenticate into applications and operating systems
- 7) Applications authorize identity and role based entitlements

Though other scenarios exist, these will do a fair job of building a case for understanding the nature of the identity management problem.

Multiplicity

First, let's look at where identity information exists. To determine the complexity of each "Use Case" identified in the previous section, let's establish a multiplier based on the number of operating systems, applications, and databases within an enterprise containing identity related information. For illustration purposes, let's assume an average Fortune 1000 company contains four (4) operating systems, three (3) data bases, and ten (10) applications (modest, if not unrealistic). Our over-simplified complexity score might appear as follows:

Identity Complexity = (7 Use Cases) X (4 OS + 3 DBMS + 10 Applications)

Identity Complexity = 119

But what does this mean? It simply means that 119 function points must now understand a common identity language (could this be SAML?). However, most of these function points have never had to communicate identity information before. This number does not even consider the complexity of attribute level (i.e., address, phone number, etc) transformation.

What can technology do?

From an overly simplified view point, a complexity score of 119 means this is a really tough technology problem (the average IT project contains approximately 12 high level function points), but given an abundance of time and money, technology could solve the engineering challenge with a combination of three approaches:

- a) **Single Identity Interface** - Providing a single interface that all user's (both administrative and employee) and applications must use when fulfilling any of the seven previously stated identity related "Use Cases" fulfills the responsibility of changing all identity storage targets and theoretically satisfies the task of enterprise identity synchronization. If you'll recall the "Provisioning" and "Policy Services" sections earlier, it should strike you that these offerings satisfy this approach to some degree. This "push approach" is a credible solution "if" all identity administration occurs through a single interface.
- b) **Synchronization (Meta-Directory)** - Synchronizing identity change events from each application, operating system, and database containing identity related data into every other database, operating system, and application, and unified central directory containing identity relevant data, can also make a serious play toward the ultimate SSO objective. This approach is credible "if" all applications, operating systems, and databases can be modified to accept a universal format



Logic Trends, Inc.
www.logictrends.com

Atlanta

1050 Crown Pointe Parkway
Suite 295
Atlanta GA 30338
office: 770.551-5050
info@logictrends.com

Dallas

Tampa

Cleveland

for user id and password and applications can be modified to accept a persistent session or token². However, today, for example, many operating systems and databases differ on what they consider acceptable user id and password lengths which creates a dilemma.

With (a) and (b) we have simplified administration and have even taken a first step toward providing a unified user id and password, However, users must still “log in” multiple times since we have not changed applications which perform their own “log in” function). This brings us to one last technology task...

- c) Modify custom applications and encourage third party applications to adopt a token (Kerberos, Tickets, SAML, PKI, etc) approach that allows applications to know when a user has already logged in. Consequently, a user is not challenged again for authentication.

Summary

It would appear that all the product and solution ingredients discussed in the first section are necessary to complete a true unified Identity solution. But will that be enough?

It's about the people, not the engineering!

If you have had the good fortune of participating in Identity Management and/or Simplified Sign-on Projects, you have learned the Holy Grail of success is not seeking the Holy Grail. Additionally, you would have learned the importance of focusing on something other than technology.

Like all projects of enterprise scope, it is the combination of...

- 1) Human habits
- 2) Comfort zones
- 3) Culture
- 4) Organizational boundaries (territory)

...that stand in the way of successful Identity Management. Make no mistake, the engineering is complicated. However, even perfect engineering will fail when faced with the human factors of habit, comfort, culture, and territory. Consequently, these factors must be addressed early and often.

Human Factors

However, even a perfect plan that embraces the need to focus on some of identity management's human challenges, will meet some overwhelming obstacles that may turn a holistic identity management strategy into a multi-year initiative:

² A persistent session or token is the media that allows multiple applications to trust that a user who authenticated previously is still authenticated. This is handled today by Kerberos Tickets, SAML, etc.



Logic Trends, Inc.
www.logictrends.com

Atlanta

1050 Crown Pointe Parkway
Suite 295
Atlanta GA 30338
office: 770.551-5050
info@logictrends.com

Dallas

Tampa

Cleveland



- 1) **Password Expiration** - Legacy users may not be able to change their passwords through a web based, third party identity management tool (since he or she does not have or care to have web access)
- 2) **Help Desk** - Call Centers and Help Desks have been provisioning accounts and resetting client server and legacy passwords for nearly two decades and must be retooled, retrained over six to twelve months and process
- 3) **Technology Interference** - Legacy environments and applications such as TSO and ROSCOE will continue to prompt the user to change expired passwords driven from RACF and ACF2
- 4) **Authentication Habits** - Tens of thousands of employees within a large corporation have an established habit of using different user ids and passwords for a variety of different applications and will not be quick to unlearn what took decades to learn.
- 5) **Territory (organization)** – IT application owners have invested much time and energy enabling authentication and authorization in many unique silos (in the absence of an enterprise identity solution) and will not be quick to risk application outages or re-assign resources focused on new features to embrace an enterprise policy services API.
- 6) **Participation Barrier** – An enterprise identity management effort will not be able to solicit participation from every user group and IT development group in defining the overall identity management road map. Consequently, when roll out time nears, countless ears will resist the change due to an innate human response...."you didn't ask me for my input, so why should I put my application at risk".

Like the technologies that define an enterprise identity management solution, human factors also are not insurmountable. However, human factors must be acknowledged up front when establishing overall time and cost expectations.

Acquiescence

Based on past project experience, flipping an "on switch" to reveal a comprehensive identity management solution within an enterprise will not happen. Of course, most IT professionals understand the value of incremental success and will not find this information enlightening. However, introducing an understanding of "human factors" with an incremental success strategy *is* essential to the success of an overall identity management project strategy.

Acceptance

It is important to first accept that human factors are slow to change. Consequently, project leaders will shy away from the human challenge and focus on technology (a common weakness in many IT projects). Understanding these two facts can present the beginning of a project road map that can succeed in large enterprises:

- 1) Human factors are slow to change
- 2) Identity Management project leaders will focus on the "safety" of technology



Atlanta

1050 Crown Pointe Parkway
Suite 295
Atlanta GA 30338
office: 770.551-5050
info@logictrends.com

Dallas

Tampa

Cleveland