



DELPHI GROUP

Identity Management Workflow - Automating A Way Out of Chaos

ID-Synch v2 by M-Tech Information Technology

October 2003

SNAPSHOT

Can Security and Business Efficiency Co-Exist?

Unfortunately, the economy continues to stagnate and most money being spent on security is for cleanup efforts after virus or worm outbreaks occur... not pro-active security and resulting business efficiency/improvement.

There are many misconceptions surrounding security - that it is: expensive, painful, does more harm than good, and results in barriers to both attackers **and** business itself. Security done well, however, streamlines operations by minimizing the likelihood of compromise to systems, and enables legitimate users to go about their business with a minimum of fuss. Identity Management (IDM) fits perfectly into this model - making systems easier to maintain by administrators, allowing users to easily access systems by making their identities consistent across all systems, enabling self-service and providing efficient tools for technical resources at all levels (from help-desk to architects) to spend less time in repetitive, manual work.

The good news is that there are **real** solutions in the IDM space, such as M-Tech's ID-Synch, that can solve points of pain for a wide variety of users, and automate a way out of time-consuming, money-wasting issues that are hindering modernization and long-term planning of efficient **and** secure information systems. M-Tech gets this point and is striving to make identity pains invisible and addressed rapidly - from customer reports ID-Synch is installed and providing value in a matter of days rather than months - enabling businesses to get a jumpstart on a reasonable Return On Investment (ROI) and freeing resources to move on to other **business-enabling** projects.

Integration, Centralization - Theory, Reality - Chaos...

There have been a number of consolidation or centralization drives to put all credential/directory services into a handful (or in theory ONE) repository. For better or worse, complete centralization has not happened, and disparate systems continue to exist for the typical reasons: expense in conversion, custom applications that are no longer well understood and may have no further benefit in being updated/connected differently, political sensitivities where systems cross boundaries in organizations, and so on.

Most organizations do not have the luxury of throwing everything out to rebuild from scratch with the most modern technologies and business practices, particularly in the current economic climate. The simple reality is that large enterprises have an extremely complex ecosystem and as with most ecosystems, radical, instantaneous transformation attempts mean further chaos is the likely result.

Defining Benefits and Problems to Solve

Features of IDM systems are typically illustrated from the end-user benefit, and that is a key component in pursuing these systems - selling benefits to individuals certainly helps create buy-in prior to purchase and during roll-out of solutions. However, the true power (and greatest ROI realization) is largely in the "back office" where efficiencies in managing large volumes of identities across a large set of systems can be more fully realized and quantified - and the risks of unmanaged or poorly managed identity can be most effectively mitigated.

To minimize errors, rapidly setup or remove accounts across a large number of systems, enable

For more information:

M-Tech Information Technology
#203, 735 - 12th Avenue SW
Calgary, Alberta Canada T2R 1J7

403 233 0740 p
403 233 0725 f

sales@mtechIT.com
www.mtechIT.com

ID-Synch v2 Highlights:

Update Operations:

Change Attributes, Create User, Delete User, Modify User, Rename User, Move, Join/Exit Groups, Reset Password, Clear Lockout

Business Processes:

Authorization Workflow, Central Management, Delegated Administration, Password Synchronization, Password Reset, Propagation

Target User Directories:

Applications, ASP/ISP, DBMS, ERP, Groupware, Hardware Tokens, LDAP, Mail, Mainframes, Midrange Systems, NetWare, Windows

SOAP-Compatible Fulfillment Engine:

Allows a standards-based connection point to modern systems

Integration Points:

Meta Directories, E-mail Systems, Call Tracking Systems, eSupport Systems, Authentication Systems, Biometric IVR Systems

Allows auto-monitoring of Systems of Record (such as HR) for any changes and automatically propagating changes throughout managed systems

Allows business users to request and authorize requests for user access to systems, auto-updating changes to user accounts upon final approval

Central and Delegated Administration allows global or departmental I.T. resources to manage any user on any system from a single point

Rapidly enables setup of new employees, contractors, partners on relevant systems

Enables cleanup of orphaned account to minimize potential damage from compromised legacy accounts

Creates consistent, standards-compliant (per organization's own standards) accounts

Ensures terminated users are handled promptly and reliably with minimal administrative overhead

both administrator and end-users the ability to reset passwords, assign new passwords, easily request new rights/privileges - those are the sorts of operations that benefit from automated systems that ensure that new employees are enabled quickly, ex-employees are quickly locked out of affected systems, and new systems are quickly populated with the appropriate user base without complicated custom integration points.

Abstraction (Identity Middleware) Works... With Proper Engineering

Systems have gotten out of control, and there is a need to restore sanity to working life. In the case of IDM, if it is a difficult proposition technically, monetarily or politically to centralize the identity store - perhaps it is possible to drape an IDM meta layer over the systems within your organization, that brings the power of centralized management without the pain of completely re-architecting or migrating all of your existing solutions to a single repository. There are many questions a buyer should ask of this Identity Middleware...

Can the solution map out all of my operational access management problems (create, delete, modify, rename, reset passwords, join/exit groups, or clear lockout)? Can it manage all of the platforms/systems in my organization (LDAP, Windows, NetWare, ERP, Mainframe, Hardware Tokens, etc.)? Can it provide all of the business processes surrounding IDM that we desire (password synchronization, password reset, propagation, central management, authorization workflow, delegated administration)? Can it address custom applications - and if so, is the approach heavy-lifting, lightweight integration, or a pipe-dream?

For areas where "single ownership" of a system may not be possible, or is distributed (by region, perhaps), ID-Synch's abilities to both centralize **and** delegate (restricted) authority enables responsibility and direct action at the most suitable level within the organization.

Watch and Learn - Hands-Off Automation

For a literal hands-off approach to IDM, ID-Synch is able to monitor a system of reference (typically a Human Resources directory) for changes (adds/deletes/renames/updates) and automatically changes the relevant settings on all systems being managed. This both speeds up the time that new employees, contractors or partners gain access, in a consistent manner, as well as rapidly **disabling** access for employees that have left the organization (voluntarily or not).

Enhancing Security, or Another Risk?

Nay-sayers of IDM claim that centralization, specifically the collapse of credentials into a single package creates far more security problems than it solves. Taken to the extreme, a potential concern on the administrator side is that if an attacker were to gain access or otherwise intrude on the IDM solution, who would know and what could be done about it? Since ID-Synch is indeed handling sensitive access information, M-Tech has taken these concerns to heart and built mechanisms to encrypt data both in storage and in transit, and the solution itself is stored on a hardened platform. In the evolving world of compliance concerns, all activities performed through ID-Synch have audit trails documenting what changes were made, by who, when, and to what systems. Even for those who are not encumbered by regulatory issues, audit trails are key to sound security operations.

Looking to the Future

Security is more important than ever before, and solutions such as ID-Synch are providing ways to reign in costs and turn spending towards more useful ends - increasing productivity and security through enforceable, far-reaching mechanisms that serve end-users, business process owners and technology teams alike. Down the road, IDM solutions should further address: auditing of rights (of existing users) according to templates, scheduling of adds/deletes (ex: contract workers), and continued Web Services/SOAP adoption as standards-based "glue." In general, these solutions should serve business needs rather than security for security's sake only. ☼



www.delphigroup.com

Delphi Group
10 Post Office Square
Boston, MA 02109-4603

(617) 247.1511
fax (617) 247.4957