

End-to-End Identity Management With Oblix and Microsoft

WHITEPAPER



Copyright © 2004 Oblix, Inc. All rights reserved

This white paper is for informational purposes only. Oblix makes no warranties, expressed or implied, in this document. Mention of third-party products within this publication is for informational purposes only and constitutes neither an endorsement nor a recommendation.

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

Software and documentation Copyright © 1996-2003 by Oblix, Inc. All rights reserved. Oblix, NetPoint, Oblix NetPoint, COREid, and the Oblix logo are registered trademarks of Oblix, Inc. NetPoint COREid System; User Manager, Group Manager, Organization Manager, IdentityXML, Certificate Processing Server (Verisign®), COREid Server, and WebPass; NetPoint Access System: Access Manager, Access Server, WebGate, and AccessGate; SHAREid, SmartMarks, SmartWalls, SmartMaps, SAML quickCONNECT, FEDERATEDid Layer, Oblix IDLink, Associate Portal Services, NetPoint System Console, NetPoint Ready Realm, NetPoint Federation Services, NetPoint Mainframe Security Connector, NetPoint SAML Services, and their logos are trademarks of Oblix, Inc. All other company and product names are trade names, service marks, trademarks, or registered trademarks of their respective companies.

Printed in the United States of America

Printing Date: January 2004

Part Number: obx9h

Oblix, Inc.
18922 Forge Drive
Cupertino, CA 95014, USA
+1 408 861 6800

European Headquarters
Atrium Court
The Ring, Bracknell
Berkshire RG12 1BW, UK
+44 1344 393 054

www.oblix.com
info@oblix.com

The Need for Identity Management

Both inside and outside the corporate firewall, identity information determines who has access to electronic data and applications. With nearly all key company data now accessible through the network, enterprises want to ensure that only authorized users have access to protected information. At the same time, companies must ensure that partners, customers, and employees can access the data and applications required to conduct business. Balancing these objectives is the challenge of identity management.

Oblix COREid® and SHAREid™ combined with Microsoft's Identity Management products provide a comprehensive solution for managing and applying identity of internal and external users in both centralized and federated identity environments. Oblix and Microsoft offer a comprehensive solution supporting the key features necessary for automated and manual administration, security, synchronization, aggregation and transformation of identity data and its application in securing access to applications and resources.

Oblix COREid identity products provide critical functionality that extend Microsoft's Active Directory®/ADAM, Identity Integration Server (MIIS), and SharePoint Portal™ to support identity based initiatives such as single sign on, regulatory compliance, identity synchronization, federation, and others. Oblix COREid wraps key features around the Microsoft infrastructure to deliver a complete enterprise identity management solution. This paper summarizes how Oblix COREid can be used to build an enterprise scale, end-to-end identity management system using the Microsoft infrastructure.

Microsoft Identity Management Products

Microsoft provides a comprehensive suite of products aimed at addressing the identity management problem at the attribute level. These products consist of Active Directory/ ADAM, MIIS, and the SharePoint portal. Oblix COREid provides the business level application that provides the security, administration, and access control features required to deploy the Microsoft infrastructure at the enterprise level. A short description of the components of this infrastructure is provided below.

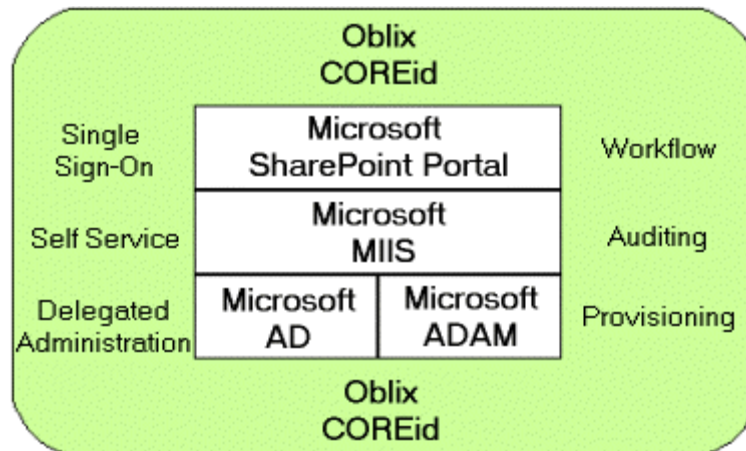
- **Microsoft Active Directory** – Active Directory® provides the means to manage the identities and relationships that make up network environments. Windows Server 2003 makes Active Directory simpler to manage, easing migration and deployment.
- **Microsoft Active Directory Application Mode (ADAM)** is a Lightweight Directory Access Protocol (LDAP) directory service that runs as a standalone user directory, decoupled from the network operating system. ADAM represents a breakthrough in directory services technology that provides flexibility and helps organizations avoid increased infrastructure costs.
- **Microsoft Identity Integration Server (MIIS)** - MIIS 2003 enables corporations to increase security and productivity while lowering IT costs. MIIS provides metadirectory and user provisioning capabilities to ensure consistent identity data across data stores. MIIS automates the process of distributing identity changes and profile updates across enterprise applications.

- **SharePoint Portal Server 2003** - SharePoint supports intelligent portals that connect users, teams, applications, and data over the Web. SharePoint operates at both the department and enterprise levels and integrates seamlessly with the desktop applications and tools used by nearly every employee.

Oblix COREid Extends the Microsoft Identity Platform

Oblix COREid wraps around the Microsoft identity management infrastructure to provide identity administration, provisioning workflow, and a complete web access control system. COREid provides features that extend the Microsoft identity management products to support the scalability and administrative requirements for large enterprises, especially within high-volume extranets. COREid has been specifically engineered to work with and extend the Microsoft infrastructure to meet today’s demanding identity management requirements. Key components include:

- **COREid Workflow** provides a sophisticated system for applying business rules and processes to identity administration and provisioning. COREid Workflow allows approvals and notifications to be routed to the proper individuals within an organization for identity events such as adding and deactivating users, or changing attribute values in a user’s profile. Within COREid Workflow, identity-based delegation and attribute security ensure that only users with appropriate rights can participate in workflow approvals. The combination of COREid, AD/ADAM, and MIIS delivers a centralized system for applying business rules to internal and external users across all applications.



- **COREid Provisioning** (available in Q2 2004) for MIIS is unique in its support for “active provisioning” directly into MIIS. Unlike other products that support provisioning indirectly through Active Directory, COREid works directly with the MIIS Metaverse to configure accounts on target systems without requiring the AD schema to be extended to accommodate the resource specific permissions or settings.. COREid Provisioning for MIIS incorporates a unique template approach that facilitates the definition of workflow processes that apply outside the AD environment. This allows target system permissions or settings to be provisioned without storing redundant information in each users profile. The combination of COREid Provisioning and MIIS provides a best of breed system for centralized administration and synchronization of identity data.

- **COREid Administration Console** is a web based tool for managing identity data contained in Active Directory and MIIS. This console is based on XSLT stylesheets for easy customization and can be modified to expose specific functionality to specific subsets of the user population.
- **COREid User Self-Service** provides self-registration and end-user self service capabilities through a web based interface. Using these pre-packaged tools, enterprises can easily extend the Microsoft AD/ ADAM and MIIS infrastructure to externally facing portals supporting large user populations. COREid self-service functions enable administrative scalability by pushing profile administration closer to the groups that manage it.
- **COREid Access System** provides a comprehensive access management and single sign on capability for heterogeneous environments. The COREid Access System supports single sign on for web applications as well as the market leading application servers including ASP.NET. COREid Access integrates with the Microsoft SharePoint Portal using the Windows Impersonation feature available with IIS6. Using Windows Impersonation, users logged in to their Windows desktops can sign on to web applications transparently.
- **COREid Auditing** – Oblix COREid provides a unique auditing framework that captures information for each identity change event for storage in a central database in real time. COREid Auditing provides a reporting tool for generating reports based on changes to user data in Active Directory as well as authentication/ authorization success and failure events.
- **COREid IdentityXML** is an XML interface that supports all of the COREid administrative functions. Using COREid IdentityXML identity administration, bulk changes and group membership checks can be performed programmatically against your identity data in Microsoft AD/ ADAM and MIIS.
- **SHAREid** is the first stand alone multi-protocol identity federation server designed and packaged for distribution to your trusted partners and organizations. SHAREid provides a standards-based approach to secure integration with your trusted partners. SHAREid provides a unique and flexible solution for integrating your identity system with other internal and external portals, data repositories, and access control environments.

Typical Projects For Oblix and Microsoft Identity Management

The depth and breadth of a combined Microsoft-Oblix solution supports a broad range of identity management initiatives, including:

- **External or Internal Portals** - COREid administration and access control features with SharePoint Portal and Active Directory bring a comprehensive solution for managing access permissions for internally or externally facing portals. The same system that can be used to manage employees is flexible enough to accommodate the differing security requirements for customers and business partners. Oblix COREid provides self-service, single sign on, workflow, and delegated administration to help portals scale to enterprise levels.

- **Global Address Book Applications** - MIIS' ability to synchronize identity information between different e-mail directories, combined with COREid's self-service and fine-grained attribute access model, gives employees or customers the ability to take control of managing aspects of their own portal applications.
- **Account Provisioning** –MIIS and COREid Workflow provide a complete metadirectory-based provisioning solution. These products combine best of breed synchronization, aggregation, and transformation at the data layer with the UI, business logic, and workflow from COREid. The result is quick propagation of identity data about newly hired employees to all relevant systems, as well as automated reversal when employees leave.
- **Security and Privacy Compliance**– Use COREid Management for determining who can view and modify identity information contained in Active Directory/ ADAM. Audit and track changes to the identity data. Generate reports using the bundled reports server.

Conclusion

For both centralized and federated identity management, Oblix and Microsoft have created a seamless set of integrated solutions addressing the data layer all the way to the application layer. Leading corporations have deployed these products to manage tens of thousands of employees/partners and hundreds of thousands to millions of customers. These companies enjoy the ease and power of a combined security solution that spans the desktop to the data center to the extranet. In addition, Oblix identity products also integrate with Microsoft products outside of the Microsoft Identity Management platform. For example, Oblix COREid also protects and manages users accessing applications in IIS, Content Management Server and Internet Security and Acceleration (ISA) Server.

To learn more about how Oblix and Microsoft deliver world-class identity solutions, please contact Oblix at:

Oblix Inc.
18922 Forge Drive
Cupertino, CA 95014
+1.408.861.6800
info@oblix.com
www.oblix.com