

White Paper

Unified Identity & Service Delivery



Leveraging unified identity & service delivery to manage identity, provision, virtualize and secure resources & services in an enterprise SOA

Executive Summary

There are many business and technology forces that are pushing information technology to deliver IT services and intellectual property (IP) resources on-demand. At the same time there are other forces that are pushing IT to provide better accountability, compliance, management and security for IT and IP resources. Traditional solutions have proven incapable of providing better accountability, compliance, management and security for IT and IP resources in that are distributed and deployed across the Internet, and moving towards a service oriented architecture (SOA).

Rethinking loosely coupled distributed deployments of tightly coupled host and client server systems puts a lot of focus on "identity" as a common element of all systems, architectures, and deployment best practices. All systems have identifying characteristics of users and resources that are used to authenticate users and authorize resources. What is needed is the ability to manage identity attributes and relationships in loosely coupled deployments and architectures, between systems and networks of tightly coupled users and resources. In such an identity "platform," network and application systems create, edit, and delete identities and apply whatever policies are specific to the system, such as workflow and access privileges. And, a distributed "identity platform" could be capable of providing identity synchronization, virtualization, integration, and policy, relationship, compliance and security services, and reporting that is complimentary to and independent of the network and application systems.

Introduction: Today's Challenges

Identity management has been practiced for a number of years. Servers have evolved from centralized host computers with closely coupled users and resources, in which an access control list (ACL) is used to authenticate and authorize access by users to resources. Network servers likewise have closely coupled users and resources but may be decentralized across a network of attached servers and client devices. The ACL of host systems evolved into a directory service (DS) capable of authenticating users, and authorizing access to network applications, files, and services.

Additionally web browsers, routers, and web servers provide transparent (virtual) point-to-point communications which bridge between tightly coupled host and network users and resources, and mobile users and remote resources, creating seamless, virtual, workgroups and social networks that span the Internet.

DS, identity management (IdM), identity and access management (IAM), single sign-on (SSO), and network access control (NAC) products extend and supplement existing network and application specific authentication and authorization services with varying degrees of success, integration and costs.

Networks, applications and web services have a variety of user and resource attributes and relationships they use to authenticate and authorize users and resources. There is no flexible, reliable and inexpensive method to provision and manage users and resources which bridges the gap between tightly coupled host and network servers, and loosely coupled, distributed, heterogeneous, systems which does not impose additional complexity and integration requirements upon Enterprise IT staff and budgets.

Today, many enterprise business processes are automated by many enterprise applications, platforms and networks. Each application, platform and network has specific authentication and authorization criteria, policies, and methodologies. Additionally, enterprise services, applications, platforms and networks have specific group, role and relationship organizational parameters. Attributes and relationships in one system are rarely duplicated in all systems, creating a patchwork of common and uncommon identity attributes and relationships across a distributed network of loosely coupled networks, platforms, applications, and services.

Business processes are organizationally grouped by job function. In other words the human resources department performs the human resources business processes, manufacturing operation performs enterprise resource planning processes, IT departments provide IT processes, and so on. And, budgets and staffing for business process services, applications, platforms and networks are managed by the enterprise department responsible for each business process.

Managing identities across and between enterprise services, applications, platforms and networks has traditionally fallen to the IT department since they were already supplying enterprise-wide network and security services. However the various business process service, application and platform owners are very reticent to give up their ability to create, edit and delete identities within their various systems.

Current solutions for user and resource identity management, provisioning and security have proven incomplete. They are complex to deploy, disruptive of established processes, provide only partial functionality and management of the problem, and are limited in their scope of coverage of business critical IP and IT resources. In other words, today's identity management (IdM), identity and access management (IAM), single sign on (SSO), proxy, network access control (NAC), and user and resource provisioning solutions provide lots of reward for tightly coupled network and application users and resources, but little reward and lots complexity and risk for the loosely coupled distributed enterprise.

The intent of current "identity" products is to serve and automate user and resource authentication, authorization, provisioning and access to critical IT and IP resources for authorized users. However, being tightly coupled to the network and application servers does not clearly delineate identities (nouns) from network and application services and transactions (verbs). For example, authentication of a user is a transaction that is performed on an identity versus a create, edit or delete, identity event. Additionally, in a tightly coupled network or application, the server acts as an identity proxy or intermediary, and all communication between users and resources is through and controlled by the network or application server.

Separating the management of identities from the management of network and application transactions removes the proxy/intermediary server from the identity management role, and frees it to manage service and application transactions more efficiently. Creating an identity intermediary or middleware platform can provide an identity repository of identity reference objects that are a superset of identity attributes and relationships of all enterprise user and resource identities. Such an identity repository can be a platform from which to synchronize identity attributes and relationships across the enterprise, while also providing a routing capability between identities to connect users and resources via a virtual directory web service of available resources users have rights.

PresenceID: an Identity "Services" Platform

- **Identity Repository** - If an identity platform repository is populated with identity attributes and relationships by the business process services, applications, platforms and networks. An identity repository can be a clearing house for identity synchronization, virtualization, management and reporting. Existing closely coupled host and network based resources can be provisioned on-demand, over a distributed network of users and resources. An identity repository can also "cleanse" identity data to remove duplicate identities, and normalize attributes and relationships. Applications and services can also make a standard web service request of the PresenceID repository asking if an identity exists, and if the identity does not exist, the requestor can then proceed to create, edit or delete the identity, as opposed to checking with each service, application, platform and network to determine the existence of an identity.
- **Identity Provisioning** - PresenceID loosely couples the services, applications, platforms and networks of an enterprise to enable user and resource identities to be provisioned and de-provisioned to authorized resources such as files, applications, web portals, and other network and web services. Identity provisioning automates a number of administrative tasks, system specific user and content provisioning, and rights administration. Additionally access control and session management, policy and role management, compliance management and reporting, software license and asset management, other management applications and appliances can be provisioned with user and resource identity attribute and relationship data.
- **Identity Synchronization** - PresenceID loosely couples the services, applications, platforms and networks of an enterprise to allow identities to be updated between services, applications, platforms and networks. Identity synchronization does not supersede the identity source system ability to control identities in their respective systems. PresenceID identity synchronization is not an authoritative identity system, but rather an enterprise identity synchronization service that depends on the identity source systems to create, edit and delete identities within their respective systems.
- **Identity Data Cleansing** - Duplicate identities can be identified and logged. Duplicate identity logs can be queried with SQL queries and sorted by system and supplied to identity source system administrators. Additionally, if an identity source system does have an automated data cleansing sub-system PresenceID can be deployed to provide duplicate names for the identity source system to delete from its data file(s). Identity data may be entered by an identity source system incorrectly by the system and/or a human operator. For example, a system operator may misspell a name, or only enter an initial for a first name, or enter an incorrect digit in a social or driver license number. PresenceID will synchronize the error, and the enterprise authoritative system will flag the error and reject it. PresenceID will then synchronize the correct data from the enterprise identity authoritative system (often an HR or payroll system).
- **Identity Healing** - Queue Manager - When an identity source system is unable to communicate with the PresenceID server (PresenceID Hub Manager) all identity provisioning and synchronization messages are put into a queue that resumes operation when the communication failures is resolved. When identity provisioning and synchronization messages resume the system is quickly brought up to date. Communication failures may be caused when systems are taken off-line for updates, upgrades, other maintenance, and when there is a communication failure due to system or internet failure.

- **Attribute Value Change (“Key Change”) Manager** - When an identity attribute (i.e. last name, address, phone number, etc.) is edited, and that attribute is shared by other identity source systems, then PresenceID will make the attribute value change and maintain its relationship with other systems. If the other systems are capable of making an attribute value edit it will be performed automatically. If on the other hand, the other system is not capable of recognizing an attribute value change as valid, a list of changes can be generated from a SQL query of a PresenceID log file and provided to the individual system administrators for manual updating.

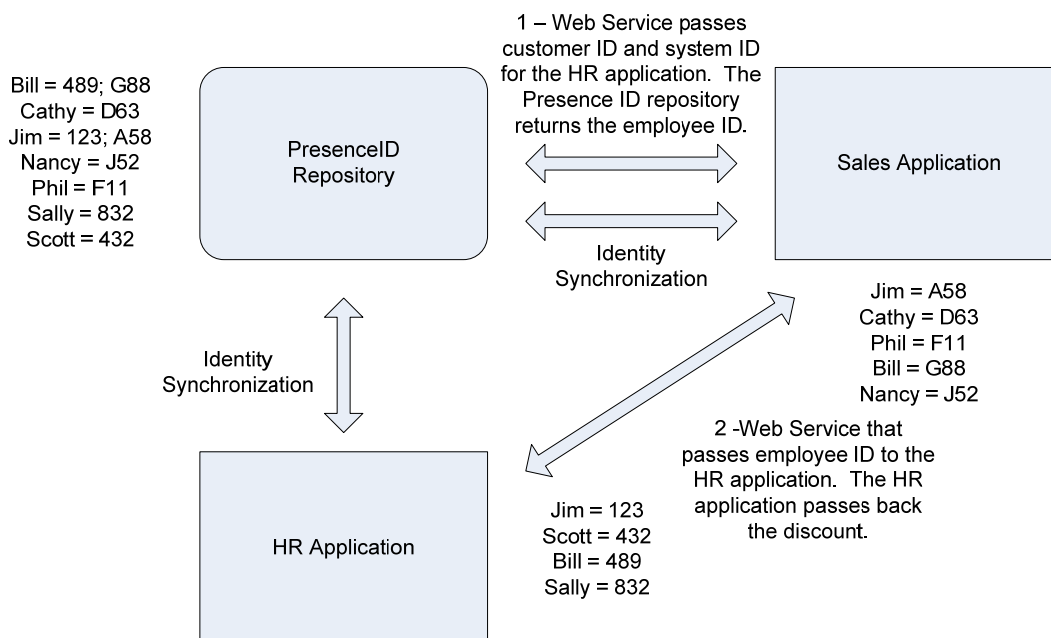
Service Oriented Architecture (SOA)

Identity Presence - The PresenceID data repository stores with each identity reference object a superset of all of the attributes and relationships used by an identity to create relationships with other identities. From a data base perspective any single identity reference object contains all of the “key” information required to create a relationship with any other identity.

A classic problem enterprises encounter is when different applications have some attributes in common and others that are unique, and data is needed from both to make a business decision.

For example, when data is required of an HR application to properly determine an employee discount rate based on title and length of employment. The HR application has four employees with employee IDs. A CRM application provides for employee discounts. The CRM application has five customers with customer IDs. PresenceID would have an aggregate of seven identities for the HR and CRM applications, and may have two of which exist in both systems.

- 1) *Classic System Integration Option 1* - extend the CRM application database to include employee information such as an employee ID. A regular CRM application process could run a query to find the “matches” between employee database and CRM database, and store the discount rate with each match.
- 2) *Classic System Integration Option 2* - Another method would be to create a remote procedure call (RPC) that the CRM application can invoke to find the appropriate discount rate. The RPC would be added to the HR application for real time response to any question about the proper employee discount by the CRM application.
- 3) *Identity Web Service* – A web service that utilizes standard web communication protocols would be an improvement for communication between the HR and CRM systems. However architecting a web service does not find the matches between the two systems, unless one or both of the data bases are extended to accommodate data from the other.
- 4) *PresenceID Unified Identity and Service Delivery* – creates an identity reference platform that provides an alternative to costly extensions of the CRM and/or HR application data bases to include the others identity keys.



The PresenceID repository contains all the keys for all identity relationships all of the time. An application can simply use its identity key to ask the PresenceID repository for the identity key of that another application uses for that same identity, through a standard web services interface.

PresenceID provides a real-time alternative to extending application databases, or running periodic jobs to replicate information between application databases. Web services allow the applications to be loosely-coupled, avoiding costly integration.

The benefits of PresenceID are obvious with even two business applications. The cost and resource savings of resolving "match" issues between applications are multiplied when the number of systems, platforms, applications, and services increases.

Legacy Integration with SOA - The PresenceID data repository contains a number of different classes of identity objects that represent users, resources (services), objects and groups. Object reference objects (ORO) may be executable software code that is executable upon demand. PresenceID provides an SOA interface service, with no modifications or custom programming to existing host, client server and distributed systems, platforms, applications and services.

An ORO could contain a script that executes a series of commands in a variety of host or client server applications, and external managed services. For example an ORO when accessed by an authorized user could execute a query of a PresenceID log file (or data warehouse), format the results into a regulatory compliance report, and email the report to a line of business executive and the enterprise compliance staff.

An ORO could also contain a script that executes a policy management application when a file is accessed from a user who has rights to it under specific conditions such as time of day, for example.

Identity Compliance Reporting

Reporting what identities have rights to access what resources is very valuable to an enterprise. PresenceID logs all identity events and stores them in log files which are in comma delimited files in a SQL compliant data base. Some of the business and IT processes that can benefit valuable identity data from PresenceID log files by executing a standard SQL query or via an application specific PresenceID Spoke Manager are:

- Regulatory Compliance & Corporate Governance
- Software License & Asset Management
- Desktop & Server Management
- Help Desk & Customer Service
- Content & Document Management & Retention
- Billing & Accounting Applications
- Web Services

Identity Provisioning & De-Provisioning

Automated Provisioning & De-provisioning - One of the most resource intensive functions IT staff perform, are provisioning users to systems, platforms, applications and services and virtual servers and machines. PresenceID can create, edit or delete an identity with any system communicating with PresenceID.

Many enterprises use contractors and part-time labor for a variety of tasks. Provisioning and de-provisioning short term, transient, and new employees can be a tedious and often inaccurate manual process. PresenceID automates and eliminates inaccuracies that often turn into security issues when former employees and contractors still have rights and privileges to internal IT resources.

And, in a SOA many users of IT resources are other applications in addition to the traditional (human) user. PresenceID can provision and de-provision user and application identities to IT resources and files to which they have rights and privileges just as accurately and efficiently as it does users.

Self-service Provisioning – User attributes fall into three general categories, personal, business and governmental. Personal attributes such as name, biometric, biographical and geographical characteristics. Business attributes can be items such as job, role, group, network ID, email address, mail stop, pay grade, etc. And, governmental attributes can be licenses and permits, social number, security clearance, etc.

Users who can provide their personal attributes from a self-service user interface (from a browser) can initiate automated provisioning processes that save valuable IT resources for other higher value processes. PresenceID provides a web based user interface for users to input and manage their personal attributes, and then provision the users to other systems such as the HR, payroll, and network systems:

- *Personal Identity Management* – biometric, biographical and geographical characteristics such as name, address, phone, personal physical characteristics, etc.
- *Rights Delegation* – users can delegate rights for a specific period of time to specific other users. Delegated rights are accessed using the delegated user's log in and password.
- *Trusted Circle* – users may name a "trusted circle" of associates that have the right to reset a user's password. Trusted circles can cut a very large percentage of the cost of help desk budgets. Some industry analysts have calculated that help desk staff spend approximately 40% of their time resetting passwords. Help desk staff resetting a users password is a security issue when the users logins and passwords are revealed to the help desk staff.

Conclusion

The power of identity-centric, service delivery, over standard Internet protocols is significant, and offers measurable business benefits to most enterprises. Nearly every enterprise faces compliance, governance, risk, technology evolution, and other business and regulatory drivers that argue for a comprehensive and effective approach to identity management, user and content provisioning, and resource access and delivery. PresenceID uses existing data base, security and web standards to provide a comprehensive unified identity and service delivery solution that compliments and integrates existing host, client server, and new distributed products and services.

Managing the complexity of the modern IT systems servicing even a modest enterprise has become one of the largest single expenses in an IT budget. And, identity products have become part of the problem because of complex and expensive integration capabilities with other systems. PresenceID simplifies identity integration using existing system APIs and data stores to communicate identity data between systems over standard web protocols as a web service. PresenceID enables SOA for existing and new architectures of IT systems.

About

PresenceID Inc. is a privately-held corporation headquartered in Salt Lake City, Utah. It was founded by identity management, security, network and data warehousing veterans. PresenceID works directly with customers, and with leading solution partners and vendors of identity, security, virtualization, solution integration and development, network management, content management and storage in mid-market and large enterprise, government, military and education environments.

PresenceID, Inc.
324 South 400 West, Suite 250
Salt Lake City, UT 84101

www.presenceid.com
(801) 363-1000