

Fischer International Identity

BUILT FOR BUSINESS... YOURS™

PRODUCT OVERVIEW

Introducing Fischer Identity™

This paper is intended for Business Analysts and others who are interested in the technical and business aspects of Identity Management in an in-house deployment. It may also be used as an introduction to *Fischer Identity Suite™: Architecture Overview (MCW-07-170)*.

Table of Contents

- 1. Synopsis..... 1
- 2. Identity Interoperability Challenges 2
 - 2.1 Fischer Interoperability Advantages 2
- 3. Fischer Identity Capabilities 3
 - 3.1 Compliance & Audit 3
 - 3.2 Federated Provisioning 3
 - 3.2.1 Rule-Based Provisioning 4
 - 3.2.2 User Self-Service Provisioning 4
 - 3.3 User Self Service 4
 - 3.4 Password Management 5
 - 3.5 Privileged Account Management (PAM) 5
 - 3.6 Federated Access Management 5
 - 3.7 Enterprise Business Roles and Role Engineering 6
 - 3.8 Interoperability / Connectivity 6
 - 3.9 Mobile Identity Management 7
 - 3.10 Multi-Organization / Multi-Tenant Operation 7
 - 3.11 Quality / Availability / Scalability 7
 - 3.12 Extending Existing IdM Solutions 8
- 4. Identity Management Procurement Models 8
 - 4.1 Outsourced Identity Management: Managed Identity Services™ 8
 - 4.1.1 Outsourced On-Premise 8
 - 4.1.2 Hosted 8
 - 4.1.3 On-Demand: Identity as a Service™ (IaaS™) Model 9
 - 4.2 Why Consider Cloud Computing Technology for Non-Cloud Use 9
- 5. Conclusion 9
- 6. References 10
- 7. Glossary 10

1. Synopsis

Identity Management (IdM) is important to managing compliance and security, and is one of the keys to preventing identity theft. Architecture is vital to addressing Identity Management (IdM) challenges for organizations of all sizes as well as for any procurement model. Architecture is also the foundation for security, privacy, usability, automation, efficiency, and all other Identity Management features. Additionally, leading analyst organizations report customer dissatisfaction with traditionally architected provisioning initiatives:

"There is a consistent message from UP [user provisioning] customers that UP products are still too complex to implement and maintain on an ongoing basis and, therefore, require too much technical support from the vendor and / or systems integrator." (Gartner)

Interoperability technology is a key requirement for Identity Management since it must typically connect many systems and applications, but it must also be lightweight so it can be implemented and maintained through business changes, i.e., no scripting and no replication of components when traversing firewalls, locations or domains. Fischer Identity features a powerful interoperability engine at its core. This is a key advantage since Identity Management is primarily an interoperability activity. Fischer's advanced architecture inherently reduces complexity and improves the usability and maintainability for implementers, administrators and end users.

Provisioning ensures enterprise workforce effectiveness and controls access to each resource to reduce the risk of unauthorized activities. Fischer's patent-pending technology ensures business flexibility while reducing skill requirements and costs. It also affords organizations the flexibility of allowing end users and their managers to initiate the provisioning process or to completely automate it. End users can improve their productivity through user-friendly interfaces that enable them to request needed resources and to reset forgotten passwords.

Compliance is a key requirement and auditors are becoming increasingly sophisticated in assessing and testing organizational controls. Fischer Identity helps organizations ensure security and compliance through preventive, detective and corrective controls. Privileged account management enables organizations to further control shared and administrative accounts, often viewed as the keys to the kingdom. This streamlines the process, speeds audits by quickly providing needed information and controls costs.

Fischer's multi-organization / multi-tenant capabilities enable unique business processes, auditing and security for each segment of your organization. All business segments can be managed centrally from a single server or in a distributed manner, and a single solution can simultaneously meet the requirements of multiple subsidiaries. Fischer Identity also supports role-based security and control for all aspects of IdM and interoperates with role engineering products for additional capabilities. Additionally, provisioning approvals and password management can be performed through mobile phones or PDAs. Of course, Fischer Identity provides quality, availability and scalability to meet the service-level requirements of all organizations including very large and complex organizations. It also provides investment protection to organizations that have already deployed IdM solutions from other vendors. Fischer Identity can typically extend existing solutions to support additional business processes and connected systems faster and more cost effectively than natively extending the existing solution.

Organizations can choose from multiple procurement models for most software, but only recently has there been a choice of models for IdM software. Technology must facilitate the business requirements of organizations rather than dictate which business choices are available. Fischer Identity is the only product that supports all procurement models, whether an organization chooses the traditional software-as-a-product model, or one of the outsourcing models discussed in this paper. With Fischer technology, you can choose the procurement model that best fits current requirements and have your investments protected if they need to change to another model in the future.

2. Identity Interoperability Challenges

Identity Management (IdM) is typically viewed as a security challenge, but it's also an interoperability challenge. Most conventional IdM offerings are composed of disparate point products such as password management, meta-directory, provisioning, and compliance that vendors acquired or developed independently to round-out their IdM suites. Because these point products have disparate designs, the solutions typically require numerous integration points, multiple administrative interfaces, invasive connectivity agents, and disparate audit log files, which compounds the IdM challenge. In fact, implementing a conventional IdM product typically requires thousands of lines of code to be written and maintained. As a result, conventional IdM technology involves longer implementation times, significantly more administration, higher-skilled resources, reduced quality, and ultimately, much higher costs. This leaves the organization with a solution that is very difficult and expensive to maintain, and repeated professional services are often required to maintain or extend the solution.

Also, though most sizable organizations operate across multiple domains, multiple locations, multiple data centers, multiple business partners, etc., traversing domains and firewalls with conventional solutions is usually cost prohibitive since it requires additional or duplicated components in addition to duplicated work. It's easy to see why implementations of conventional suites have significant failure rates as well as why many organizations are replacing their suites or are acquiring competing components to extend their solutions.

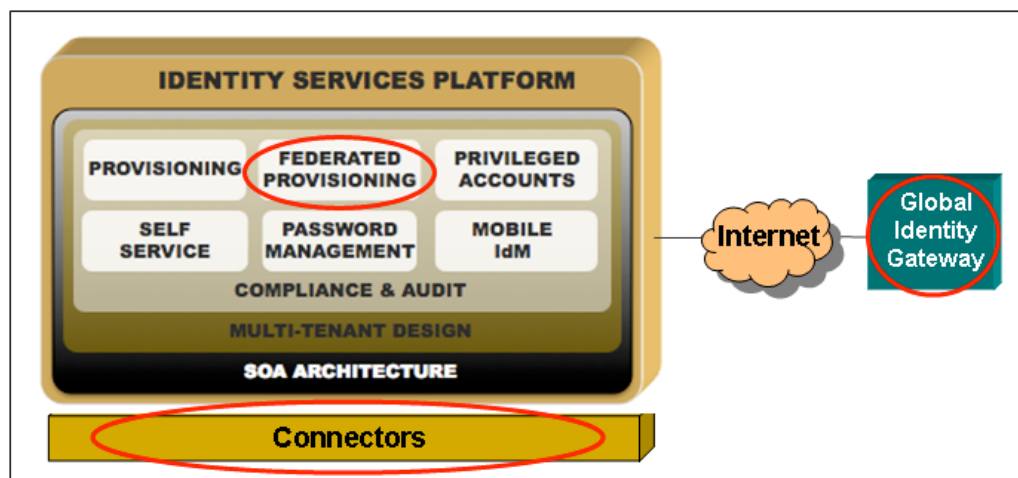


Figure 1: Fischer's Global Identity Architecture™

2.1 Fischer Interoperability Advantages

Fischer Identity is the only IdM product built to address the interoperability challenges of Identity Management. Fischer's Global Identity Architecture™ (GIA) was designed as a single solution and is built on service-oriented architecture (SOA). GIA enables rapid implementation and supports constantly-changing business requirements. It is also the keystone required for federating identity management and extends far beyond SOA to ensure that organizations have a robust, easy-to-use technology that solves very complex problems.

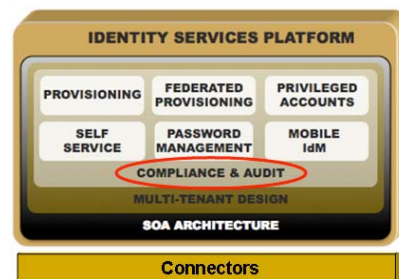
As depicted in Figure 1, Fischer provides a contemporary approach to IdM architecture and design. It has unified compliance, united administration and control, shared resources, and global connectivity. All facets of the solution work seamlessly across enterprises, domains and firewalls. Fischer Identity was designed as an interoperability technology, and is the only IdM product that eliminates the need for coding and scripting regardless of the complexity of the business process. This greatly reduces time for creating and modifying solutions, simplifies problem determination and debugging, and improves quality and reliability.

3. Fischer Identity Capabilities

This section discusses the key capabilities of Fischer Identity to meet business challenges.

3.1 Compliance & Audit

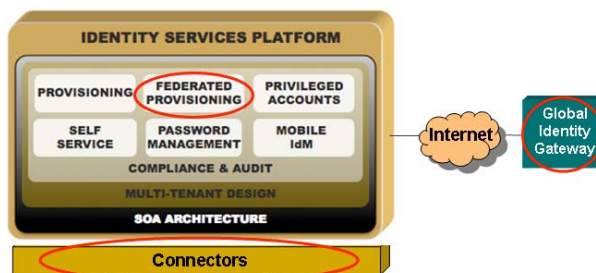
Fischer Identity helps organizations of all sizes to ensure the security of their assets and to comply with a wide array of regulations such as Sarbanes-Oxley, HIPAA, J-Sox, PIPEDA, GLBA and the European Privacy Directives. The solution has compliance incorporated throughout the architecture rather than as an add-on feature or product. This superior approach to compliance enables customer to:



- Automate preventive, detective and corrective controls to enforce business policies and to avoid problems such as separation of duties conflicts.
- Detect and remediate compliance violations either as they occur, on demand or periodically.
- Simplify audit preparation and enable auditors to quickly validate compliance through the comprehensive audit database.
- Prove "who had access to what, and when," including systems and data such as financial records, protected health information (PHI) and other sensitive information.
- Detect non-compliant conditions, alert appropriate personnel, and, optionally, automatically remediate exceptions.
- View summary and detailed exception information in a standard reports and database views.
- Automate attestation process workflows.
- Manage privileged and shared accounts such as root accounts, etc.

3.2 Federated Provisioning

Federated provisioning enables organizations to ensure enterprise workforce effectiveness by providing appropriate resources when required. It controls who has access to each resource, including IT resources such as accounts and privileges as well as non-IT resources such as credit cards and badges. Provisioning ensures that each person has access to the correct resources and that no one can access resources unless specifically authorized. Société Générale is an example of an organization that did not properly provision or deprovision its resources. They did not always deprovision accounts when employees were terminated. In 2008, one of their stock traders used these "orphan" accounts to amass a loss of 4.9 billion euros without being detected. Federated provisioning would have prevented this problem.



Fischer's unique architecture enables control of resources for people who are located anywhere across enterprises, domains and firewalls. The provisioning (and deprovisioning) process is initiated 1) through user-friendly self-service pages, 2) via requests from line managers, or 3) automatically as events occur on connected systems. Each provisioning workflow can optionally require approvals and can notify appropriate persons about the status and progress of events.

Fischer's patent-pending technology reduces skill requirements, complexity and costs. The solution reduces implementation time by approximately half and enables less-expensive personnel to perform implementation and reduces support requirements, which significantly reduces costs. Packaged solutions reduce implementation time even further. A key reason for this advantage is that Fischer Identity is the only solution that has eliminated the requirement for scripting or coding.

Fischer eliminates the requirement for any special expertise to reside at or to travel to each remote location. Implementation and ongoing management of connectivity to resources at remote locations can be managed from a single location. This is possible since Fischer's Global Identity Gateway can be deployed either as an appliance or as software while web-services security safely enables remote management.

3.2.1 Rule-Based Provisioning

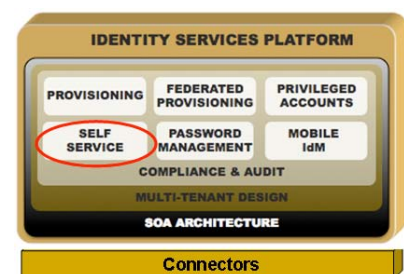
Business events such as hiring a new employee can automatically initiate the provisioning process. By and large, rule-based provisioning provides the most rapid and most cost-effective method to assuring the appropriate levels of access for all users. When Human Resources enters information about a personnel action in an HR system like Oracle-PeopleSoft or SAP, appropriate processes are automatically initiated. Each organization's rules specify who should be granted access to each resource based on factors such as location, membership in a specific department, or other factors. Some organizations automatically route pending actions for approval by designated persons before the resources are actually granted. Rule-based provisioning can also be combined with user self-service provisioning when not all rules have been defined. Both rule-based and request-based provisioning can reach any level of granularity as the most detailed entitlement requests can be sent to administrators for fulfillment.

3.2.2 User Self-Service Provisioning

End-user interfaces can provide a fast and easy method for end-users and managers to initiate the provisioning process by selecting resources for themselves or for their employees / business partners using business terms rather than using IT terminology. Some organizations refer to this process as role management. Requests are automatically routed for approval by designated persons before the resources are actually granted. Requesters and beneficiaries can be automatically kept apprised of the status of their requests through email. Self-service typically requires a shorter implementation time and can be used as a stepping stone to achieving rule-based provisioning.

3.3 User Self Service

Fischer Identity delivers robust self-service capabilities through a variety of user-friendly interfaces that improve workforce effectiveness by enabling end users, managers, approvers and others to quickly and productively request resources, reset forgotten passwords and easily perform a variety of other tasks. Interfaces include web browser, Fischer iFly mobile access, the login and password change mechanisms of Microsoft Windows LAN Server and Novell NetWare LAN Server and a secured LAN account that acts as a password kiosk that can be used from any LAN-attached workstation.

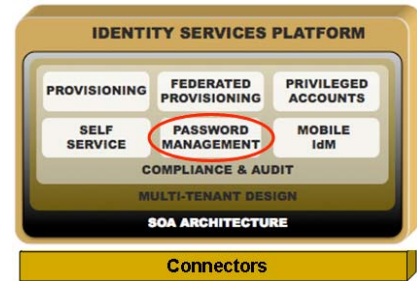


Fischer's out-of-the-box web interface can be configured to provide appropriate levels of access to each user to meet your organization's requirements for self-service provisioning and other tasks. Additional customization is possible to meet unique requirements. Other abilities include:

- Eliminating passwords in emails: Fischer Identity provides a unique interface for securely distributing new account credentials to users without exposing passwords to anyone. Initial passwords can be securely created through a challenge-response mechanism that can be pre-populated with information from any connected systems. This can also replace the non-secure facilities commonly used for extranet password resets that send user passwords via email.
- Self-service provisioning and role management as described in sections 3.2.2 and 3.2.1.

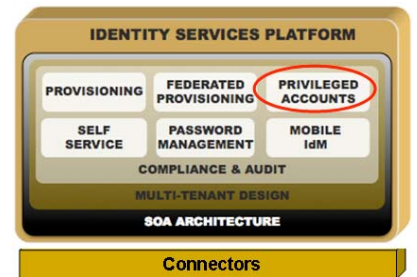
3.4 Password Management

Fischer Identity enables users to securely reset their forgotten passwords through a variety of interfaces without calling the Help Desk, which improves the user experience and reduces costs. It flexibly enforces each organization's unique password policies and enables users to automatically use the same password for accounts on multiple systems. To further save time, the organization can specify that any number of systems is grouped together so that a single password change alters passwords for all systems in the group. Password Manager also speeds, simplifies and secures Help Desk operations by providing a single interface for Help Desk representatives to change passwords for all systems and applications. Without this interface, Help Desk representatives are currently required to learn multiple proprietary interfaces, which also require multiple administrators to create numerous Help Desk accounts with just the right privileges for each connected system. When using native interfaces, help desk administrators are also at risk of catastrophic errors since they have more privileges than required.



3.5 Privileged Account Management (PAM)

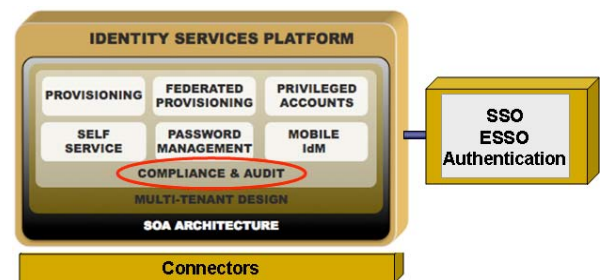
Privileged and shared accounts are a growing security concern, especially to organizations with ongoing corporate governance and compliance initiatives. Fischer Identity controls the “keys to the kingdom” by managing administrative and shared accounts that are often highly privileged, but cannot be traced to an individual user. These accounts are frequently the targets of identity thieves and others (both insiders and hackers) because they can bypass controls to access or destroy sensitive information without being traced.



Auditors recognize that unmonitored, uncontrolled access to privileged accounts leave organizations wide-open to privacy breaches, fraud and identity theft. For instance, the \$250 million loss at TJ Maxx was performed via access to shared accounts. As a result, auditors are increasingly issuing adverse findings for organizations that have not implemented controls to mitigate this risk. Unlike standalone PAM products, Fischer Identity also controls the actual privileges associated with each account. The end result is complete control and auditing of exactly who can perform administrative and other high-privilege functions, during which periods of time, and who approved their privileges. It also simplifies auditing by showing which high-privilege accounts were active and which were not active at any point in time.

3.6 Federated Access Management

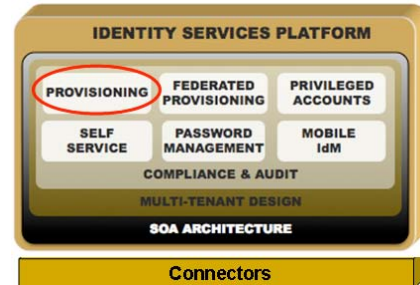
Fischer Identity complements federated access management (SAML, Liberty Alliance, WS-Federation) by enabling robust provisioning capabilities that are not addressed by federation such as individual account creation, approvals, escalation, changes in access rights, etc. Fischer's interoperability with access management has two facets. First, Fischer Identity can automatically provision accounts and privileges on SSO / ESSO and other authentication servers so that each user receives appropriate privileges. Second, users of Fischer Identity can be authenticated through web single sign-on (SSO) and enterprise SSO (ESSO) or other authentication products. It provides out-of-the-box interoperability with virtually any third-party products such as IBM TAM, Entrust GetAccess, RSA ClearTrust, Imprivata OneSign, etc. Interoperability is via SPML, Web services and other methods. Strong authentication to Fischer interfaces using smart cards, biometrics, etc. is supported through this interoperability.



Fischer's Global Identity Architecture allows organizations to fully manage all provisioning requirements and processes across multiple domains and organizations. The result is a single (federated) login and a single point of audit, administration and compliance that spans enterprises, domains and firewalls.

3.7 Enterprise Business Roles and Role Engineering

Enterprise business roles represent groups of persons who perform similar functions and need similar resources to complete their duties. Though not required by the Fischer solution, most organizations choose to use at least some enterprise business roles for identity management. For Identity Management, the pertinent aspects of roles are who qualifies for a role and what resources should be provided to role members. Once defined, Fischer Identity can automatically identify who qualifies for a role (based on characteristics like job title, location, department, temporary workgroup, etc.) and automate provisioning and tracking the resources. Fischer Identity provides an interface for less-technical persons to quickly and easily define roles without requiring programmers.



Roles can also be managed through the self service interface so that end users or managers can request role privileges as well as requesting more granular entitlements. Requests can require approval by one or more persons before being granted automatically or before administrative actions are authorized.

Role engineering enables organizations to analyze, audit, cleanse and periodically recertify their populations of roles, accounts, and entitlements, and to determine the optimum role management models based on their goals and priorities. They can validate, audit, and refine their roles and entitlements before moving them into production. This approach helps ensure that privileges and policies can be monitored, planned, developed and maintained to meet each organization's goals in a changing environment. Fischer Identity can bidirectionally share user role membership information with role engineering tools through entries in a data repository.

3.8 Interoperability / Connectivity

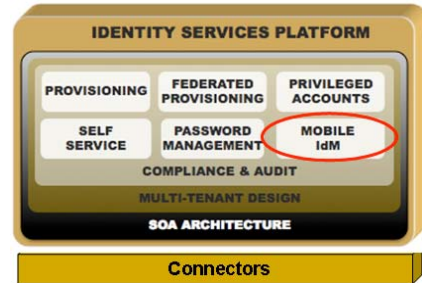
Identity Management implies interoperability, yet conventional identity products cannot provide simple and widespread interoperability between systems that are across data centers or across enterprises. Fischer provides an interoperability services platform and a wide array of connectors designed to quickly bring disparate systems together.



Even more important than Fischer's ability to connect out-of-the-box with hundreds of different systems and applications is how the connectors are created and what they accomplish. All functions except the actual connections with other systems are performed in the engine, which eases implementation and support. Fischer's unique approach enables data mapping to be performed once and easily reused across multiple connected systems, which speeds implementation and reduces costs. Gartner has stated that this is a very positive approach since it eliminates the need to manage scripts or configurations on multiple servers, possibly at multiple locations.

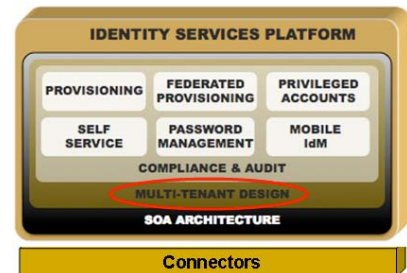
3.9 Mobile Identity Management

The Fischer iFly mobile client delivers password-management and provisioning approval functions to mobile devices such as PDAs and telephones so that organizations can choose the best individuals to approve provisioning requests without regard to whether the person travels or not. Workflows do not need to be delayed when approvers travel. Fischer was the first to introduce this technology, which caters to the growing mobile workforce.



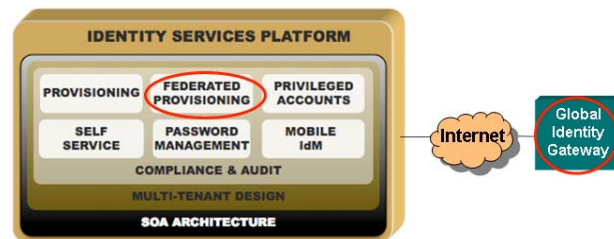
3.10 Multi-Organization / Multi-Tenant Operation

Regardless which sourcing model is chosen by your organization, Fischer's multi-organization / multi-tenant capabilities enable unique business processes, auditing and security for each segment of your organization. All business segments can be managed centrally from a single server or in a distributed manner. This ability enables new acquisitions to be brought on more rapidly and allows subsidiaries to be divested faster. It also provides the ability to manage SLAs by controlling the priorities of resources given to your business processes, subsidiaries, business partners, etc. Multi-organization / multi-tenant capabilities also enable service providers to deliver more cost-effective services. Please refer to the following section for additional detail: Advantages of Solutions Handling Cloud Computing.



3.11 Quality / Availability / Scalability

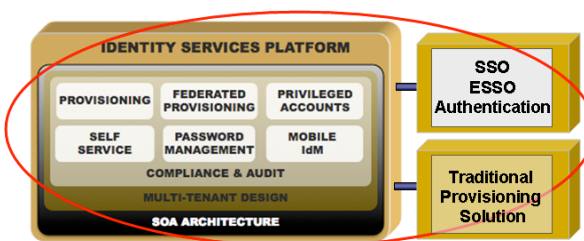
While not unique to Identity Management, quality, availability and scalability are vital to the success of any critical IT solution. Eliminating scripting, promoting reuse and using visual tools not only reduces time and cost, but improves quality as errors are both easier to avoid and easier to detect. High availability is a core component of Fischer Identity so that there's no single source of failure. The strong problem determination and recovery are vital to meeting service-level agreements (SLAs). Also, hot backup servers at remote locations can be maintained for organizations that need non-stop operations.



Fischer Identity has unlimited scalability and can grow either by using a larger processor or by clustering multiple processors. Also, resources can be used more efficiently since separate instances of business workflows can be executed simultaneously on multiple processors with the assurance that all tasks are also processed in the right order.

3.12 Extending Existing IdM Solutions

The drawbacks of changing or extending traditional IdM solutions are legendary. Many organizations run solutions that they don't dare change as thousands of lines of scripting can be affected by seemingly innocuous business changes. Instead, some organizations add manual processes to support changing business needs. Eventually, the IdM solution and the added makeshift processes can no longer be supported and an expensive solution replacement is required. In contrast, the flexibility of Fischer Identity enables organizations to keep their investments in existing IdM solutions while expanding their capabilities to support additional business processes and additional connected systems. Fischer Identity can interoperate with other IdM solutions so that minimal or no changes are required on the existing solution and end users don't need to be impacted. As discussed in the next section, Fischer Identity also protects the investments of organizations that choose to change their procurement models in the future.



4. Identity Management Procurement Models

Technology must facilitate the business requirements of organizations rather than dictate which business choices are available. Organizations can choose from multiple procurement models for most software, but only Fischer enables a full choice of procurement models for IdM software, whether an organization chooses the traditional software-as-a-product model, or one of the outsourcing models discussed below. With Fischer technology, organizations can choose the procurement model that best fits their current needs and have their investments protected if they need to change to another model in the future.

4.1 Outsourced Identity Management: Managed Identity Services™

Outsourcing is an umbrella term for when an organization transitions the management, operation, accountability and responsibility for specific business operations or processes to another organization. There are several different models that fall under this umbrella as described in the following sections.

4.1.1 Outsourced On-Premise

The common denominator of on-premise outsourcing is that the Service Provider furnishes the service on the client's premises. Ownership of the infrastructure assets (hardware, software, networks, etc.) can be flexible, with either the Service Provider or the Client owning some or all of the infrastructure assets. Software requirements for this model are consistent with those of the traditional software-as-a-product model. The complexity of the clients' enterprise drives the requirements for the software. For example, a large manufacturing organization with many different data centers and business partners would require software that can securely, seamlessly, and simply cross domains to enable both intra-enterprise and inter-enterprise business processes.

4.1.2 Hosted

In hosted outsourcing, the software being operated by the Service Provider is physically located at the Service Provider's data center. As with the outsourced on-premise model, ownership of the infrastructure assets (hardware, software, networks, etc.) can be flexible, with either the Service Provider or the client owning some or all of the infrastructure assets, but the assets are typically dedicated to a single client organization. Technical requirements for this model typically depend on the location of managed systems. If the connected systems are also hosted in the same domain at the same Service Provider's data center, then the requirements are similar to the outsourced on-premise model; however, if the connected systems are located at the client's site, then the requirements are similar to the on-demand model.

4.1.3 On-Demand: Identity as a Service™ (IaaS™) Model

In the on-demand / IaaS™ model, a Service Provider owns the infrastructure and hosts the software in its own facility to make it available to clients over a network via the Software as a Service model. On-demand solutions often employ some type of multi-tenancy (one-to-many) approach where at least some of the assets are shared among multiple clients. This shared approach is possible because the service is typically more productized with standardized options and less customization for each client. Connected systems would normally reside at the client's locations, so that by definition, they are not in the same domain as the IdM software and the IdM software must quickly and cost-effectively support cross-domain operations when on-boarding new clients.

The technology that enables Service Providers to provide identity management from the cloud also benefits end-user organizations choosing other procurement models, as described in the next section.

4.2 Why Consider Cloud Computing Technology for Non-Cloud Use

Why should end-user organizations care about which technology Service Providers choose? Costs, functionality and risk management. Service providers are on the hook for meeting service-level agreements by reliably addressing their clients' business requirements at competitive prices, and managing their own costs to be profitable. Many of their reasons for choosing Fischer technology also benefit end-user organizations that choose alternate procurement models.

- Flexibility – both up front and down the road – Fischer enables you to change procurement models if your business procurement strategies change.
- Service providers demand the lowest TCO – their due diligence helps you identify the lowest-cost solution.
- Much easier and faster to traverse boundaries such as locations, data centers, business partners, etc., and no expertise is required at remote locations, which reduces cost and time for implementation and ongoing support.
- Simplified interfaces and elimination of scripting enable the use of lower-cost personnel as well as faster implementation and business changes.
- Enables managing priorities for business processes, subsidiaries, business partners, etc. to meet internal SLAs.
- Enables unique business processes, auditing and security for different parts of your organization, yet these can all be managed centrally or in a distributed manner.
 - New acquisitions can be brought on faster.
 - Subsidiaries can be divested faster.
- Enables business workflows to be executed simultaneously on multiple processors in a high-availability environment with the assurance that work is also processed in the right order.

5. Conclusion

Identity Management (IdM) is vital to managing compliance and security, but traditional IdM solutions are complex, take a long time to deploy and can be very difficult to change, leading to limited flexibility and high costs. Flexible technology is required to address the ongoing challenges of implementing, maintaining and sustaining a world-class IdM solution, both within and across enterprises. Fischer's interoperability engine delivers flexibility and control to ensure fast, simple, and widespread connectivity across all enterprise systems, applications, and end-to-end business processes. Fischer Identity protects existing IdM investments through cost-effective extensibility and by enabling organizations to change their procurement models.

Fischer's Global Identity Architecture reduces skill requirements while improving quality, business agility and costs. Secure connectivity and high availability extend across multiple domains to cost-effectively connect additional systems. Preventive, detective and corrective controls improve compliance and reduce costs; for instance, proactively enforcing separation of duties assures compliance policies while automating privileged account management recaptures the "keys to the kingdom." iFly mobile interface for provisioning and password management improves the quality of decisions and the user experience.

Fischer Identity is the only IdM solution that can be implemented using any procurement model: SaaS, hosted, outsourced on-premise, and software-as-a-product. The same solution supports a wide range of business sizes from the small to medium businesses to the largest multinational corporations.

6. References

Gartner. Witty, R. J. & Allan, A. & Wagner, R. (2006) Gartner Magic Quadrant for User Provisioning, 1H06.

Gartner. Desisto, R.P. & Paquet, R. (2006) How to Evaluate SaaS Architecture Model Choices.

Forrester. Cser, A. (2008) Identity-Management-As-A-Service.

7. Glossary

Compliance (regulatory compliance) – the process of complying with regulations like SOX, HIPAA, GLBA, PIPEDA, etc. The common requirements for almost all regulations are the ability to prove that financial or confidential systems and data have been protected, that there is a process for authorizing who can view / create / change / delete the resources, and that only authorized persons can actually access the resources.

Data cleansing – the process of ensuring that (typically historical) data is correct.

Deprovisioning – removing resources from people who are no longer authorized for them, including revoking access to IT accounts / privileges as well as collecting physical assets such as PCs and badges.

Domain – a group of networked computers and devices with common rules and procedures that are administered as a unit. Typically, anytime a firewall is crossed, another domain is required.

ESSO – enterprise single sign-on – SSO to non-web applications in addition to web applications.

Federated Provisioning – provisioning resources across multiple domains, either across enterprises or within a single enterprise.

Federated Access Management – an arrangement among multiple enterprises that lets subscribers use the identification data from one enterprise to obtain access to the networks of all enterprises in the group.

GIA – Fischer's Global Identity Architecture.

GIG – Fischer's Global Identity Gateway.

Global Identity Architecture™ – Fischer's architecture that securely extends all facets of Identity Management across domains including user provisioning, workflows, policy management, approvals, password management, self service, connectivity and compliance.

Global Identity Gateway – Fischer's Java-based gateway that enables the Global Identity Architecture. It can be deployed either as an appliance or as software.

IAAS™ - Identity as a Service™.

IAM – identity and access management.

Identity and Access Management – includes provisioning, password management, access management (SSO, ESSO, WAM, authentication) and compliance activities related to identity.

Identity Management – includes provisioning, password management and compliance activities related to identity.

Identity as a Service™ model – providing identity management services in the outsourced Software as a Service model using technology that is optimized for the managed services environment.

IdM – identity management.

Orphan account – an IT account that is not assigned to any valid user, usually as a result of failing to deprovision an account when a person left the organization.

Password Management – managing the ability to reset forgotten passwords as well as the ability to change passwords.

Provisioning – providing or removing resources to persons who need them. Resources can be IT resources like user accounts and permissions or they can be physical assets like laptops, badges and credit cards.

Recertification (attestation) – the act of validating that a person should continue to have access to a resource that has already been provided.

Regulatory Compliance – the process of complying with regulations like SOX, HIPAA, GLBA, PIPEDA, etc. The common requirements for almost all regulations are the ability to prove that financial or confidential systems and data have been protected, that there is a process for authorizing who can view / create / change / delete the resources, and that only authorized persons can actually access the resources.

Service-oriented Architecture – a collection of services that communicate with one another. The communication can involve either simple data passing or it can involve two or more services coordinating some activity.

SOA – service-oriented architecture.

SSO – (web) single sign-on – the ability to enter one's credentials once for multiple applications.

WAM – web access management.

Fischer International Identity
3073 Horseshoe Drive South
Naples, Florida 34104
+1 239-643-1500
www.FischerInternational.com



Built for Business... Yours™.

Document MCB-08-401B: July, 2009

©2007-2009 Fischer International Identity, LLC. All rights reserved.

Fischer International, Fischer International Identity, Managed Identity Services, Managed Identity Services Technology, Identity as a Service, IaaS, the Fischer International Logo, Global Identity Architecture, Built for Business...Yours, and all other Fischer product or service names are the trademarks and/or registered trademarks of Fischer International Identity.
