

Approaches to Enterprise Identity Management:

Best of Breed vs. Suites



Contents

- 1 Introduction** **1**

- 2 Executive Summary** **1**

- 3 Background** **2**
 - 3.1 Enterprise Identity Management 2
 - 3.2 Enterprise IdM Infrastructure Components 3
 - 3.3 Enterprise IdM Technical Components 4

- 4 A Best of Breed Approach** **5**

- 5 A Suite Approach** **5**

- 6 Points of Integration** **7**

- 7 Integration Value and Complexity** **10**

- 8 Managing Integration Risk** **11**

- 9 Hitachi ID Integrations** **12**

- 10 Summary** **13**

1 Introduction

Growing awareness of a variety of different types of enterprise identity management applications, combined with consolidation of identity management software vendors, are leading many organizations to wonder whether they would be best served by either a suite of products from a single vendor, or a combination of best of breed products from multiple vendors.

This is an important decision, which would be well served by a deeper understanding of the benefits and drawbacks of each approach: suite vs. best of breed.

The remainder of this document differentiates suite from best of breed approaches, and strives to shed light on the business variables that should drive a decision to pursue one or the other.

2 Executive Summary

In this document, the set of possible integrations between IdM components is reviewed, in terms of business value and implementation difficulty.

The conclusion of this analysis is that:

- Some integrations are both valuable and hard to implement.
- Suite vendors, many of whose products were derived from corporate acquisitions, are no more likely to provide the critical valuable, hard-to-implement integrations than best-of-breed vendors.
- Organizations should evaluate integrations between IdM infrastructure components in the lab, rather than assuming either that suite vendors offer fully integrated solutions, or that best-of-breed vendors do not offer integrations between IdM components. (Both of these assumptions are false.)

3 Background

3.1 Enterprise Identity Management

Enterprise Identity and Access Management (IAM) is defined as a set of processes and technologies to effectively and consistently manage modest numbers of users and entitlements across multiple systems. In this definition, there are typically significantly fewer than a million users, but users typically have access to multiple systems and applications.

Typical enterprise identity and access management scenarios include:

- Password synchronization and self-service password reset.
- User provisioning, including identity synchronization, auto-provisioning and automatic access deactivation, self-service security requests, approvals workflow and consolidated reporting.
- Enterprise single sign-on – automatically filling login prompts on client applications.
- Web single sign-on – consolidating authentication and authorization processes across multiple web applications.

Enterprise identity management systems leverage basic identity infrastructure, such as directories.

Some identity management applications are relevant to both enterprise and B2C deployments. This includes web single sign-on (WebSSO), extranet access management (EAM) and single-directory administration.

Enterprise IAM presents different challenges than identity and access management in Extranet (B2C or B2B) scenarios:

Characteristic	Enterprise IAM (typical)	Extranet IAM (typical)
Number of users	under 1 million	over 1 million
Number of systems and directories	2 – 10,000	1 – 2
Users defined before IAM system is deployed	Thousands	Frequently only new users
Login ID reconciliation	Existing accounts may have different IDs on different systems.	Single, consistent ID per user.
Data quality	Orphan and dormant accounts are common. Data inconsistencies between systems.	Single or few objects per user. Consistent data. Dormant accounts often a problem.
User diversity	Many users have unique requirements.	Users fit into just a few categories.

In short, Enterprise IAM has fewer but more complex users. Extranet IAM has more users and higher

transaction rates, but less complexity.

3.2 Enterprise IdM Infrastructure Components

As mentioned above, there are several primary components of an enterprise IdM system, beyond the underlying user databases and directories:

- **Password management:**

Password management systems externalize administration of authentication factors out of individual applications, into a shared infrastructure.

This typically includes password synchronization, password reset, administration of Q&A profiles used to authenticate users during password reset, and may also include administration of other authentication factors, such as hardware tokens, PKI certificates and biometric samples.

- **User provisioning:**

User provisioning systems externalize administration of user accounts and profiles out of individual applications, into a shared infrastructure.

These systems typically include a consolidated administration system, delegated administration, self-service workflow to enable business users to directly request and authorize changes on target systems, consolidated reporting, and some access audit.

- **Meta directory:**

Meta directories synchronize user data between multiple systems. Different systems may be authoritative for different pieces of information, such as unique IDs, e-mail addresses, phone numbers, etc. Changes in a system of record are propagated to target systems.

- **Enterprise SSO:**

E-SSO systems provide a primary point of authentication, where a user is first identified and validated, and subsequently feed a user's login IDs and passwords into applications launched by the user. E-SSO reduces the number of times that a user must re-authenticate during a single workstation login session.

- **WebSSO / EAM:**

WebSSO systems externalize user authentication from multiple web applications. Users sign into the WebSSO infrastructure first, and are then able to sign into one or more web applications without having to re-authenticate. Typically, WebSSO systems capture a user's validated identity in a web browser cookie, and provide that ID to each application in an HTTP header.

EAM systems extend WebSSO by defining central policy for what data and systems a user may access. This may be done by filtering the URLs that a user may access, or by providing an API that applications use to determine, at run time, whether a given user is entitled to access a given function or data.

3.3 Enterprise IdM Technical Components

Enterprise IdM products, while they may be different in function, can share some technical components:

- **Credentials:**

Credentials are whatever one user or program provides to a system to sign in. On most systems, credentials come in the form of a login ID and password. Other identifiers may be e-mail addresses or employee numbers. Other authentication factors may include a pass code generated by a hardware token, a PKI certificate or a biometric sample.

- **Agents:**

Also known as connectors, these enable a shared IdM infrastructure to manage users and passwords on other, existing systems.

- **JOIN Data:**

Also known as login ID reconciliation, this is the data that connects user objects on different systems to one another, to form an enterprise-wide profile of login accounts and other objects that belong to a single user.

4 A Best of Breed Approach

Best of breed vendors include Hitachi ID for user provisioning and password management functions, Microsoft for meta directories, Oblix for WebSSO/EAM and Citrix for E-SSO.

These vendors typically provide significantly greater functionality in their segment of the IdM functionality, as well as easier deployments and lower TCO. These advantages stem from:

- A singular focus on a smaller set of features.
- The reliance of these vendors on customer success stories, and consequently:
 - A deeper understanding of customer IdM requirements.
 - Greater commitment to ensuring positive customer outcomes.

Pure-play vendors cannot rely on huge sales and marketing teams to deliver revenues. They must make customers happy.

5 A Suite Approach

Suite solutions from vendors such as IBM, Novell, CA and Sun tend to include most or all of the enterprise IdM components described in [Subsection 3.3](#) on Page 4.

Each of the suite vendors also offer a directory, however as directories are all standards-compliant using LDAP, directory integration does not present any integration risks.

The suite vendors largely built their suites through a combination of in-house development and acquisitions, so the fact that a single vendor sells the entire suite does not mean that all the components integrate smoothly, or even at all.

Some components of each suite may be limited, as well. For example, the password management component may have no facility for access to self-service from the login prompt, and the suite may have no actively managed user enrollment process or distributed entitlements audit capability.

Suites do tend to provide a consolidated management console, and in some cases a consolidated logging system, useful for troubleshooting.

The quality and total cost of ownership of the components of each suite varies:

- Directory products from any of these vendors are capable and scalable, but some have architectural limitations. For example, only directories from Microsoft and Novell can be easily queried for a list of groups to which a given user belongs, without forcing the server to access every object in the tree.
All of the major directory offerings deploy quickly and easily, and in fact good quality directory products have become a commodity.

- Most of the meta directory products are capable of integrating with popular systems – Windows, NetWare, LDAP and DBMS servers. Many of them have limited connectivity to mainframes, ERP applications, less popular mail systems and custom applications.

At least one meta directory (Novell DirXML) offers the advantage of real time operation, but at the expense of installing invasive local agents on every connected system – a significant increase in complexity and cost.

All of the meta directory products in IdM suites depend on the consistent, reliable presence of anchor attributes on every directory, using which user objects across multiple systems can be linked. Since such anchor attributes frequently do not exist, deployments cost and timeline are often significantly impacted by a pre-requisite manual effort to populate such an attribute (e.g., employee ID, consistent login ID, GUID, etc.) on every system.

- Most of the WebSSO / EAM products from suite vendors are capable, and certainly all of them perform the basic function of externalizing authentication from multiple web applications, and providing some granularity of central authorization control, but none of them is as powerful, scalable or flexible as the WebSSO products from market leaders Oblix and Netegrity.

While none of the WebSSO products is difficult to deploy, configuration of complex administration workflows and integration with many applications and a portal can introduce cost and delay. This is true of both suite and best of breed products.

- The password management capability in all of the suites is quite limited – typically self-service password reset, authenticated by a small number of user-defined questions, accessed from a web browser. They are generally missing most of the other features of a mature password management system, such as access from a locked-out login prompt, access from a telephone, transparent password synchronization, help desk password reset, help desk ticketing integration, connectivity to a broad arrange of target system types or managed user enrollment.

The net result here is that suite password management products are far less capable, and require significantly more manual effort to configure, as compared to best-of-breed products.

- The user provisioning component in each of the suites – self-service workflow, consolidated security administration and delegated administration is technically functional but very difficult to deploy.

Every user provisioning system from the suite vendors requires significant role engineering – defining roles to capture every possible mix of user entitlements, and classifying users into those roles. Role engineering in a large, dynamic and complex corporate environment, as is normal in most enterprise organizations, is almost impossible to successfully complete, and very likely impossible to maintain over the long term.

The workflow engines in the provisioning offerings from the suite vendors are functional, but require manual configuration, using a flow charting GUI, for each security transaction. Since real-world user provisioning systems may expose thousands of security transactions to users, workflow administration tends to be very time consuming and costly.

The net result of these challenges is that the suite vendors have far more licensees than production deployments of their user provisioning systems.

- Most of the suite vendors include a first generation enterprise single sign-on component. These products store user passwords in a central database, and are used to launch other applications and feed login ID and password keystrokes into their login screens.

E-SSO products are typically costly to acquire, costly to deploy and costly to maintain.

6 Points of Integration

Not every organization needs every identity management function. This reduces the number of integrations between separate IdM functions in a given organization.

For those IdM functions that are deployed, there are clear points of integration as illustrated in the following table:

Table 1: Points of Integration between Enterprise IdM Functions

System	Password Management	User Provisioning	Meta Directory	Enterprise SSO	WebSSO / EAM
Password Management	-	(1) Share agents, share JOIN data	(2) Share agents, share JOIN data	(3) Re-encrypt SSO credentials after PW reset	(4) WebSSO front-end to PW system, WebSSO PW target
User Provisioning	(1)	-	(5) Add target types	(6) Provision credentials after creating logins	(7) Manage WebSSO users, fulfill EAM workflows
Meta Directory	(2)	(5)	-	(8) Provision credentials after creating logins	(9) Manage WebSSO users, fulfill EAM workflows
Enterprise SSO	(3)	(6)	(8)	-	(10) Share authentication
WebSSO / EAM	(4)	(7)	(9)	(10)	-

From Table 1, we see that there are ten possible integration points between the five main types of Enterprise IdM applications that an organization may deploy. Most organizations will deploy only a subset of these applications, and so require only a subset of the possible integrations between those applications.

The nature of each of the integrations in Table 1 bears further consideration. Some integrations are easy to construct, including by the organization deploying an IdM infrastructure, while others are very complex, requiring vendor assistance. Also, while some integrations provide significant added value, others do not.

1. Share agents, share JOIN data

Integration between: password management and user provisioning.

Agents, either remote or local, are the connection between an enterprise IdM system and target systems. Clearly, an agent that can validate current and reset new passwords, as well as creating, updating and deactivating users, can be used by both a password management and user provisioning system.

In products where target system integration is difficult, sharing agents between functional components is a good way to save time and money. In products where target integration is rapid and requires low ongoing maintenance, this integration makes sense, but is not a major contributor to reducing project TCO.

JOIN data is what connects user objects on different systems back to individual owners. Without JOIN data, it is impossible to provide password synchronization, reset or consolidated user administration.

A major component of deploying any Enterprise IdM system is to construct and maintain JOIN data across target systems. Password management systems are normally the first to be deployed, since they are simplest and provide immediate ROI. Accordingly, it makes sense for other systems, including user provisioning, to take advantage of the JOIN data assembled during deployment of the password management system.

2. Share agents, share JOIN data

Integration between: password management and meta directory.

Since password management is most often deployed first, it makes sense to leverage its JOIN data in deploying a meta directory.

In case a meta directory is deployed first, it makes sense to leverage its target system connectivity when subsequently deploying a password management system.

3. Re-encrypt SSO credentials after PW reset

Integration between: password management and enterprise single sign-on.

E-SSO systems manage a set of encrypted credentials to multiple systems and applications. These credentials are normally encrypted using a key derived from each user's primary login password.

When a password management system resets a user's primary login password, the user will be unable to regenerate the old ESSO encryption key, and so will lose his credentials. Integration is therefore required between simultaneously deployed E-SSO and password management systems, to re-encrypt E-SSO credentials after each password reset, so that users will not have to re-enroll their E-SSO credentials after a password reset.

4. WebSSO front-end to PW system, WebSSO PW target

Integration between: password management and web single sign-on.

Most password management systems are web-based, and a WebSSO system can front-end authentication into the password management system – at least for routine password updates and user enrollment.

WebSSO systems most often use a password for initial authentication, and this password can be in scope for a password management system's synchronization and reset services.

5. Add target types

Integration between: user provisioning and meta directory.

Modern user provisioning systems tend to have connectivity to many more types of target systems than contemporary meta directory products. Consequently, it makes sense to leverage a user provisioning system's agents to extend the reach of a meta directory to new types of systems and applications.

6. Provision credentials after creating logins

Integration between: user provisioning and enterprise single sign-on.

Enterprise single sign-on systems maintain a set of credentials for each user, to every system and application into which that user signs on.

User provisioning systems create and modify login accounts on the same systems.

As a result, it makes sense for user provisioning systems to write updates into an E-SSO's credential database or directory after each create-user and deactivate-user operation, to eliminate the need for separate user enrollment in the E-SSO system.

7. Manage WebSSO users, fulfill EAM workflows

Integration between: user provisioning and web single sign-on.

User provisioning systems are intended to be a single point of administration for every login ID on every system in an organization. Accordingly, it makes sense for the user provisioning system to be able to manage users on the WebSSO application, just as it does on every other application, system and directory.

In case an organization prefers to manage users through the WebSSO's identity management infrastructure, that infrastructure will require connectivity to multiple types of target systems, which is not normally available through the WebSSO application. This creates a second type of integration, where the WebSSO application manages the change request / approval process, and the user provisioning system acts as a fulfillment engine to implement approved user administration operations.

8. Provision credentials after creating logins

Integration between: meta directory and enterprise single sign-on.

This is essentially the same integration as between user provisioning and enterprise single sign-on, except that users are created and deleted as a part of the data synchronization process, rather than consolidated, delegated or self-service workflow of a user provisioning system.

9. Manage WebSSO users, fulfill EAM workflows

Integration between: meta directory and web single sign-on.

This is essentially the same integration as between user provisioning and web single sign-on, except that users are created and deleted on the WebSSO system as a part of the data synchronization process, rather than consolidated, delegated or self-service workflow of a user provisioning system, and the meta directory fulfills change requests authorized by the WebSSO's workflow engine.

10. Share authentication

Integration between: enterprise SSO and web SSO.

Where both an enterprise single sign-on system and a web single sign-on system are deployed, it makes sense to authenticate the user once, and enable access to both legacy and web applications.

7 Integration Value and Complexity

As mentioned earlier, there are ten possible integration points between the five main types of Enterprise IdM applications that an organization may deploy. These integrations can be conveniently classified by value and complexity as shown in the following table.

Table 2: Difficulty and value of integrating Enterprise IdM components

Difficulty Value	Simple	Complex
Low	4 and 10 in Table 1.	6 and 8 in Table 1.
High	7 and 9 in Table 1.	1, 2, 3 and 5 in Table 1.

The business impact of the integration value / complexity analysis in Table 2 can be interpreted as follows:

- There are four high-value, high-complexity integrations that must be provided by the IdM product vendor(s). These are: 1, 2, 3 and 5 in Table 1.
- There are two high-value, low-complexity integrations that can be implemented in the field, if the vendors do not supply them out of the box. These are:
7 and 9 in Table 1.
- There are two low-value, high-complexity integrations that can be implemented if the respective vendors support them, or simply ignored if they are not provided out of the box:
6 and 8 in Table 1.
- There are two low-value, low-complexity integrations that can be implemented in the field if vendors do not provide them out of the box, but have only a small impact on enterprise IdM architecture:
4 and 10 in Table 1.

8 Managing Integration Risk

Regardless of whether the various IdM components are acquired from a single or multiple vendors, some integrations between the components will be required, and of those, some will be complex to integrate.

To mitigate integration risk, it is important to ask the vendor(s) to characterize the high-value integrations, and to demonstrate the high-value, high-complexity integrations in the lab. These integrations are repeated here:

- **High-value, low-complexity integrations – describe:**

- Integration 7 in Table 1: provision users to a directory, from a user provisioning system, where they will be used by a WebSSO/EAM system.
- Integration 9 in Table 1: provision users to a directory, from a meta directory, where they will be used by a WebSSO/EAM system.

- **High-value, high-complexity integrations – demonstrate:**

- Integration 1 in Table 1: Share agents and JOIN data between a password management and user provisioning system.
- Integration 2 in Table 1: Share agents and JOIN data between a password management and meta directory system.
- Integration 3 in Table 1: Re-encrypt E-SSO credentials after password resets. Pre-enroll E-SSO credentials during password changes processed by a password management system.
- Integration 5 in Table 1: Share agents and JOIN data between a meta directory and user provisioning system.

Other integrations, while nice to have, are unlikely to impact project success or scope.

9 Hitachi ID Integrations

Hitachi ID offers an identity management suite. Though functionally broad, this suite does not encompass every possible enterprise IdM function.

In order to expedite customer deployments, and minimize customer risk, the Hitachi ID suite comes with a broad range of pre-built integrations with other enterprise IdM components, as follows:

- Integration 1 in Table 1 – Hitachi ID Password Manager and Hitachi ID Identity Manager share agents and user profile data.
- Integration 2 in Table 1 – Password Manager can either populate JOIN data into a directory, as it is acquired, where any meta directory can leverage it as a set of anchor attributes; or Password Manager can leverage JOIN data in an existing Microsoft ILM deployment using the ILM WMI API.
- Integration 3 in Table 1 – Password Manager can re-encrypt credentials in the Citrix Metaframe Password Manager or in the SAP Portal product after each password change. This cryptographic integration supports both interoperability and expedited E-SSO deployment.
- Integration 4 in Table 1 – Password Manager is primarily a web application, and can be configured to trust any WebSSO infrastructure, by specifying a suitable HTTP header, to authenticate inbound users.
- Integration 5 in Table 1 – Identity Manager includes a generic Microsoft ILM management agent, which enables Microsoft ILM to target new types of systems through Identity Manager, using native Identity Manager agents. This extends the reach of Microsoft ILM to a much broader set of platforms and applications.
- Integration 6 in Table 1 – Identity Manager can automatically populate E-SSO credentials for Citrix Metaframe Password Manager after creating new users.
- Integration 7 in Table 1 – Identity Manager can manage users in Oblix COREid, Netegrity SiteMinder, RSA ClearTrust and Entrust getAccess through their APIs. It can also manage LDAP users in any directory, including any attributes, for integration with these and other WebSSO/EAM systems.
Identity Manager also includes a SOAP API, which enables the workflow engines in a EAM product to terminate with provisioning actions against a variety of target systems, using Identity Manager agents.
- Integration 8 in Table 1 does not involve any Hitachi ID product.
- Integration 9 in Table 1 does not involve any Hitachi ID product.
- Integration 10 in Table 1 does not involve any Hitachi ID product.

10 Summary

There are only a modest number of integrations between the various components of an enterprise identity management architecture.

The set of integrations relevant to a given organization will depend on the set of IdM functions that the organization deploys. Of these, some will be complex to develop, while others are very simple. Some create significant added value, while others offer only minor convenience.

The fact that suite vendors sell most or all of the components of an enterprise IdM architecture does not guarantee that the various points of integration, and in particular the high-value, high-complexity integrations, are either available or work well in their suite. What is certain is that suite vendors offer significantly reduced functionality in some IdM functions.

Similarly, best of breed vendors may in some cases, and not in others, provide seamless integration with one another. They can be relied upon, however, to provide the maximum possible value, and lowest TCO, for individual IdM functions.

Organizations designing an enterprise identity management architecture should consider ahead of time what integrations they will require, and validate that solutions being considered do provide these integrations. Those integrations that are both high value and difficult to implement should be tested in a lab prior to product purchase.

As a best of breed vendor, Hitachi ID has endeavored to pre-build a wide set of integrations with other products in the enterprise IdM market. Prospective Hitachi ID customers are encouraged to validate these integrations prior to making a purchasing decision.