

© Hitachi ID Systems, Inc.



Hitachi ID Management Suite

Release 6.0
Frequently Asked Questions

Contents

- 1 What is Version 6.0 of the Hitachi ID Management Suite? 1**
- 2 What are the major features of the Hitachi ID Management Suite? 1**
- 3 Which components of Hitachi ID Management Suite are refreshed with Version 6.0? 1**
- 4 Do the components of Hitachi ID Management Suite 6.0 integrate with Hitachi ID Password Manager? 2**
- 5 How does Version 6.0 differ from previous releases? 2**
 - 5.1 New or Improved Features 2
 - 5.2 Updated Product Architecture 3
- 6 On what kinds of systems can the Hitachi ID Management Suite connect manage users, identity data, privileges and passwords? 4**
- 7 What kinds of back-end databases can Version 6.0 use? 4**
- 8 How many users can Hitachi ID Management Suite scale to? 4**
- 9 What is the cost of the Hitachi ID Management Suite? 5**
 - 9.1 License Model 5
 - 9.2 Total Project Cost 5
- 10 How can prospective partners and customers get an evaluation copy of Hitachi ID Management Suite 6.0? 6**
- 11 Can customers deploy Hitachi ID Management Suite 6.0 themselves, or are services always required? 6**
 - 11.1 Hitachi ID Services 6
- 12 Where and when is training for architects, product installers and project managers offered? 7**
- 13 What kind of companies use Hitachi ID software? 7**
- 14 How does the Hitachi ID Management Suite benefit organizations that deploy it? 8**
- 15 Is there an API into the Hitachi ID Management Suite workflow engine? 8**



16 Are there performance metrics for the Hitachi ID Management Suite?	8
17 How does Hitachi ID Management Suite differ from competing products?	9
17.1 Unique Features	9
17.2 Scalability	11
18 How will Version 6.0 of the Hitachi ID Management Suite reduce the need for implementation services?	13

1 What is Version 6.0 of the Hitachi ID Management Suite?

Version 6.0 is the latest release of the Hitachi ID Management Suite, available to Hitachi ID customers starting in February 1, 2009. It is a comprehensive solution for onboarding new users, deactivating access for departing users and managing identity and privilege data throughout each user's life cycle in an organization.

2 What are the major features of the Hitachi ID Management Suite?

Hitachi ID Management Suite is a complete identity management solution that enables organizations to more securely and efficiently manage the user lifecycle across enterprise applications and systems.

Hitachi ID Management Suite is designed to efficiently create, manage and deactivate user objects, identity attributes and security privileges across multiple applications in medium to large organizations. This is done using a combination of automation and self-service:

- Automation propagates changes from one system to another.
- Workflow invites business users to participate by completing their own profiles, authorizing changes and reviewing the current state of users and privileges.
- Consolidated management enables security staff to manage access with a user-centric, rather than application-centric view.
- Password synchronization and enterprise single signon reduce the number of passwords that users must remember and type.
- Reports enable auditors, security officers and system administrators to analyze current state and review historical changes.

A rich set of connectors are included, to easily integrate with over 70 kinds of systems and applications, and to manage authentication factors including passwords, Q&A profiles, biometric samples, OTP devices, PKI certificates and smart cards.

3 Which components of Hitachi ID Management Suite are refreshed with Version 6.0?

Version 6.0 includes the following components:

1. Hitachi ID Identity Manager (ID-Synch™) – Automated Onboarding, Synchronization and Deactivation
2. Hitachi ID Access Certifier (ID-Certify) – Periodic Review and Privilege Cleanup
3. Hitachi ID Group Manager (ID-Access) – Self-Service AD Group Management

4. Hitachi ID Org Manager (ID-Org) – Distributed Relationship Management

4 Do the components of Hitachi ID Management Suite 6.0 integrate with Hitachi ID Password Manager (P-Synch™)?

As pointed out in the previous question, Hitachi ID Management Suite 6.0 includes all of the identity management components of Hitachi ID Management Suite, but does not refresh the password management products, including Hitachi ID Password Manager.

An integration with Hitachi ID Password Manager is included in Hitachi ID Management Suite 6.0, however. This integration notifies Hitachi ID Password Manager of new and deleted users and login IDs in real time. This enables Hitachi ID Password Manager to manage passwords on new login IDs immediately after they are created.

Hitachi ID plans to release new versions of the password management products in Hitachi ID Management Suite later in 2009, using the new platform in Hitachi ID Management Suite 6.0.

5 How does Version 6.0 differ from previous releases?

5.1 New or Improved Features

Hitachi ID Management Suite 6.0 is a major release, with changes to almost every component of the product. Notable changes include:

1. Infrastructure changes:

- (a) The internal data store moves from DBF files to the customer's choice of an Oracle or Microsoft SQL Server.
- (b) Support for Unicode in user identifiers and attributes.
- (c) A new workflow API (application programming interface), allowing organizations to write custom onboarding applications, where Hitachi ID Management Suite tracks requests through approval and execution.

2. Automated provisioning, identity synchronization and deprovisioning:

- (a) A code-less identity synchronization engine, that organizations can quickly configure to keep personal data in sync between multiple systems and applications.
- (b) A new attribute priority mechanism, allowing each integrated system to be authoritative for just a subset of user profiles.
- (c) A completely new auto-provisioning / auto-deprovisioning system, which aggregates detected changes on a per-user basis and executes business logic in response to those change events. The new system (ID-Track) is much easier to configure than previous approaches.

3. Enhanced support for role-based access control (RBAC) and policy enforcement:
 - (a) Persistent role assignments to users.
 - (b) Support for calculated role changes.
 - (c) Segregation of duties policies are now built-in and enforced for all change requests.
 - (d) An exception management system tracks approved policy violations.
4. Access certification has been redesigned:
 - (a) Certification of users with role assignments is simplified, replacing multiple fine-grained privileges with single role checkboxes.
 - (b) Certification highlights new and previously approved violations to segregation of duties policies.
 - (c) The certification process is more flexible and user friendly.
5. Licensing / feature inclusion:
 - (a) Hitachi ID Org Manager and Hitachi ID Group Manager are built into the base Hitachi ID Identity Manager license.

5.2 Updated Product Architecture

The internal architecture of Hitachi ID Management Suite Version 6.0 is completely revised from previous releases. All Hitachi ID Management Suite components, including user interface screens, reports, service programs and command-line / batch processes access the database using the same architecture:

1. Client component calls a client wrapper library.
2. The client wrapper library communicates with a Hitachi ID Management Suite database service using an IPC. This may be shared memory (same server, very fast) or TCP/IP socket (remote server, encrypted communication using a shared key).
3. The Hitachi ID Management Suite database service authenticates clients, checks what they are allowed to see/do and invokes stored procedures to read from and write to the database.
4. Stored procedures, installed on the relational database back end (e.g., Microsoft SQL Server or Oracle Database Server), access data in the local schema and return results.
5. Calls to stored procedures which insert, delete or update records are forwarded by the database service to its replicating peers, so that each database instance may be kept up to date.
6. Data returned by stored procedures is passed back to the calling program.

This architecture is advantageous for several reasons:

1. Using stored procedures rather than direct SQL calls significantly improves performance while leaving open the possibility of future schema changes.

2. Using a Hitachi ID Management Suite database service to front-end the physical database enables robust access controls and easy-to-manage database replication.
3. Wrapping data calls in an encrypted protocol enables secure configuration in a distributed environment, over untrusted network segments.

In addition to the above data access architectural changes:

1. The product source code has been entirely revised and is Unicode-ready.
2. A new SOAP API is available, exposing the entire workflow system to external applications.
3. A new infrastructure has been introduced for automated processes. Whereas the old system (ID-Compare) compared lists of users on exactly two systems, the new system (ID-Track) aggregates detected changes on a per-user basis, from all data sources, and executes business logic for each user with changes. Moreover, ID-Track uses the new workflow API to directly submit requests to the workflow service.

6 On what kinds of systems can the Hitachi ID Management Suite connect manage users, identity data, privileges and passwords?

The Hitachi ID Management Suite includes connectors to over 70+ kinds of systems. A full list of supported target system types is available at:

<http://Identity-Manager.Hitachi-ID.com/technology/platform.html>

7 What kinds of back-end databases can Version 6.0 use?

The Hitachi ID Management Suite replicating data service can be configured to use any of the following SQL database engines as its physical data store:

- Oracle 10g, Enterprise Edition, R2.
- Microsoft SQL Server 2005, Enterprise Edition.
- Oracle 10g, Express Edition, R2 (free download from <http://oracle.com/>).
- Microsoft SQL Server 2005, Express Edition, with Advanced Services (free download from <http://microsoft.com/>).

8 How many users can Hitachi ID Management Suite scale to?

Hitachi ID Management Suite is an appropriate solution for managing internal users in organizations with as few as about 1,000 and as many as about 500,000 users. It is assumed that in internal deployments,

users have many identity attributes (40+) and a typical user has many login IDs (typically 2 to 20 each).

In Extranet deployments, Hitachi ID Management Suite can be used to manage millions of users, since they often have much simpler user profiles. It is assumed that Extranet users have just one user object, typically in an LDAP directory, and fewer than 20 identity attributes.

9 What is the cost of the Hitachi ID Management Suite?

9.1 License Model

Hitachi ID Management Suite pricing is based on the number of users (people, not login accounts). This includes all features and support for all target systems. A one-time purchase grants customers the perpetual right to use Hitachi ID Management Suite.

Customers are encouraged to, over time, extend their deployment of Hitachi ID Management Suite to manage new target systems and to activate new features, at no additional charge.

Customers may run as many Hitachi ID Management Suite servers as required, to provide high availability, redundancy and a test/QA environment, at no additional charge.

Please contact your Hitachi ID sales representative or e-mail sales@Hitachi-ID.com for a price quote, as this will vary based on the number of licensed users.

9.2 Total Project Cost

Hitachi ID customers can expect the following Hitachi ID Management Suite project costs:

1. Hitachi ID Charges:
 - (a) Hitachi ID Management Suite Software License Fee, one-time perpetual right to use, based on the number of users, includes all features and all platforms. There are no additional charges for running multiple servers, or backup copies.
 - (b) Hitachi ID Management Suite Annual Support and Maintenance, required at time of license and annually thereafter in years 2 and 3, after which time maintenance is an optional purchase.
 - (c) Optional fixed price professional services from Hitachi ID to implement Hitachi ID Management Suite.
2. Other Direct Hitachi ID customer Expenses:
 - (a) Server hardware and operating systems for Hitachi ID Management Suite.
 - (b) Licenses for the back end database engine (Microsoft SQL Server or Oracle).
 - (c) If Hitachi ID Phone Password Manager (ID-Telephony) is used, Dialogic hardware cards will be required.

3. Hitachi ID customer Soft Costs:

- (a) Internal resources to manage the project and to implement and roll out Hitachi ID Management Suite.
- (b) Ongoing costs to manage Hitachi ID Management Suite, including maintaining steady state (minimal), as well as adding new features and platforms (typical).

10 How can prospective partners and customers get an evaluation copy of Hitachi ID Management Suite 6.0?

Please download, print, sign and fax back an evaluation agreement form from the following URL:

http://Password-Manager.Hitachi-ID.com/evaluate/psynch_trial_license.pdf

Once this is done, please fill in the evaluation request form at:

<http://Identity-Manager.Hitachi-ID.com/cgi-bin/evaluate>

11 Can customers deploy Hitachi ID Management Suite 6.0 themselves, or are services always required?

While deployment without assistance is certainly possible, most of Hitachi ID's enterprise customers purchase a fixed-price, defined-deliverables deployment service, which may include on-site or remote control installation of all functionality and assistance with initial deployment.

11.1 Hitachi ID Services

Identity Management (IdM) products are installed across the enterprise infrastructure and have an impact on systems, directories, applications, user support, HR, corporate security and audit. To realize the benefits of an IdM solution, organizations must exercise care in selecting both technology products and integration services, to meet the needs of all these stake-holders.

In addition to industry-leading products, Hitachi ID offers design, implementation and training services to our customers. Hitachi ID solution delivery services rely on a standard methodology, optimized over hundreds enterprise-scale IdM deployments. Our methodology replaces expensive consulting with automation and self-service wherever possible, enabling Hitachi ID to deliver the lowest-cost IdM deployments available.

Hitachi ID services are available strictly on a fixed-cost, fixed-deliverables basis, eliminating cost overruns and transferring risk from our customers to Hitachi ID.

Hitachi ID takes pride in our track record with medium to large deployments, attested to by our many satisfied, referenceable customers. Our services staff bring significant technological expertise, product knowledge and implementation experience to each engagement.

Utilizing Hitachi ID's solution delivery methodology ensures rapid deployment and high user adoption. The Hitachi ID professional services team works closely with customers from project inception to full production deployment, to ensure success. Once in production, Hitachi ID's technical support team takes over, providing high quality, responsive assistance to all live installations.

12 Where and when is training for architects, product installers and project managers offered?

The following processes and tools are available to provide training and knowledge transfer to Hitachi ID customer staff:

- Formal training classes for administrators.
- Informal knowledge transfer during product installation and configuration.
- CBT, such as on-line help and animations, for users.

Introductory and advanced Hitachi ID Identity Manager training is available. These are 5-day courses are regularly scheduled at Hitachi ID's Calgary location and can also be set up at customer locations. The price is \$1,000 per person. Discounts for multiple attendees are available. These courses run four times annually.

On-site training is also available.

Recordings of past training sessions are available to Hitachi ID customers at no charge.

Topics in the introductory course include:

- Introduction
- Installation
- The central console
- The account management console
- The workflow request process
- Plug-ins

Customers also receive a sample of training materials culled from prior deployments that can be modified for their own purposes.

13 What kind of companies use Hitachi ID software?

Hitachi ID solutions have been deployed by over 780 organizations world-wide, with a combined total of over 9.8 million end users. Hitachi ID customers range from medium sized companies and organizations, with as few as about 1,000 employees, to very large deployments, impacting up to about 1 million users. Hitachi ID has customers in many industries, located in many countries, as described here:

<http://Hitachi-ID.com/aboutus/customer/>

14 How does the Hitachi ID Management Suite benefit organizations that deploy it?

Hitachi ID Management Suite delivers several concrete business values:

- Improved user productivity, due to reduced wait for new and updated systems access and fewer authentication problems.
- Lower security administration cost, as the bulk of user administration is automated or delegated to business users and password resets are either eliminated or resolved with self service.
- Enhanced security, as inappropriate access is terminated quickly and reliably.
- Regulatory compliance, including the ability to audit access rights globally, to ensure that only appropriate users have access to sensitive systems and data.

These benefits, combined with technology built for rapid deployment, yield ROI (return on investment) more quickly than any other identity management software on the market.

15 Is there an API into the Hitachi ID Management Suite workflow engine?

Yes, one of the key features of Version 6.0 is the introduction of an extensive Workflow API. The Hitachi ID Management Suite workflow API allows integrated programs to:

- Submit new change requests, to create, modify, enable, disable or delete users on one or more systems.
- Search for existing change requests.
- Approve, reject or cancel open requests.
- Add authorizers to and remove authorizers from requests.
- Update request contents.
- Search the identity cache for users matching defined criteria.

16 Are there performance metrics for the Hitachi ID Management Suite?

Hitachi ID Management Suite is extensively stress tested prior to each release. Following are some performance metrics that illustrate high throughput in the most computationally expensive process: periodic auto-discovery of users, groups and group memberships on target systems.

The following tests are carried out on commodity Intel server hardware – single CPU, dual core, 2GB RAM, SATA disks. The target systems were Microsoft Active Directory and SunONE LDAP. The internal database was Oracle 10g, Enterprise Edition on the same server as Hitachi ID Management Suite.

Number of users:	10,000	100,000
Number of managed groups:	10,000	100,000
Number of target systems:	2	2
Number of login IDs per user:	2	2
Total number of login IDs:	20,000	200,000
Number of identity attributes per login ID:	40	20
Total number of attributes loaded:	800,000	4,000,000
Average number of group memberships login ID:	50	25
Total number of group memberships loaded:	1,000,000	5,000,000
Time required to list the above data and load it into the Hitachi ID Management Suite internal database:	20 minutes	4.5 hours

These short run times mean that it is both practical and recommended for customers to perform auto-discovery nightly.

17 How does Hitachi ID Management Suite differ from competing products?

17.1 Unique Features

A number of innovative features incorporated into Hitachi ID Management Suite are not available with any other identity management product:

- **Self-Service Login ID Reconciliation**

Initially introduced in Hitachi ID Password Manager and later productized in Hitachi ID Automated Discovery (ID-Discover), this patent-pending process combines auto-discovery and managed enrollment with a verifiable method for users to connect their non-standard login IDs to their enterprise-wide profile.

In organizations with non-standard login IDs, self-service login ID reconciliation eliminates many months from the timeline and cost of an enterprise identity management system's deployment.

- **User Provisioning Without a Privilege Model**

Real-world user entitlements are often difficult to model. Roles and rules break down when a given set of privileges applies to just a few users or unique individuals.

Hitachi ID Identity Manager is uniquely designed to function, delivering value and improving security, without a formal privilege model. Deployment is not held up while the organization undergoes a multi-year role engineering project, as often happens with other user provisioning systems.

- **Access Certification**

Without a formal privilege model, short of termination, it is hard to say when a given privilege is no longer required by a user and so should be revoked. As discussed earlier, formal privilege models are challenging to construct at best and may delay the deployment of a user provisioning system for years, if not indefinitely.

This creates a problem: users continue to retain privileges that may have been appropriate in the past, but are no longer consistent with their responsibilities.

Hitachi ID Access Certifier is a unique solution from Hitachi ID for periodically activating business stake-holders: managers, application owners and group owners, to review detailed user rights and to flag inappropriate privileges for deactivation. Hitachi ID Access Certifier is a key to IT support for regulatory compliance.

- **Dynamic Workflow**

As user provisioning deployments scale up to include hundreds of target systems and thousands of managed groups and attributes, it becomes infeasible to define separate workflows for every possible kind of security request. Flowcharting/drawing tools are great for demos, but have no place in a large scale, manageable user provisioning system.

Hitachi ID Identity Manager's workflow engine is built from the ground up to scale to this level of complexity. A single change authorization process is built right into Hitachi ID Identity Manager and customers are asked to make real business decisions, rather than drawing pretty pictures.

Whose authority is required for this change? Are these user attributes valid and self-consistent? What login ID should be assigned to this new account? What resources should a user with these attributes be given? How often should authorizers be reminded to act? What authorizers should be activated when some do not respond?

These are meaningful questions to businesses that deploy a user provisioning system. The Hitachi ID Identity Manager dynamic workflow engine is unique in that it requires only that organizations answer these questions, in as general a manner as possible. Individual workflows are a thing of the past.

- **Self-Service OrgChart Construction**

In most organizations, security changes are authorized in part or in full by managers. In order to deploy a user provisioning workflow engine, it is necessary to relate every user to at least one manager, in order for the system to identify the right authorizers. User/manager relationships are also useful in escalations and access certification.

Most organizations have poor quality, incomplete and obsolete OrgChart data. Hitachi ID Org Manager, built into Hitachi ID Management Suite and bundled with Hitachi ID Access Certifier, automates a unique process that allows organizations to delegate regular construction and maintenance of this data to all managers, eliminating both project delay and significant ongoing cost as this data is assembled and updated.

- **Network Resource Access Management**

Large organizations operate hundreds of file servers, thousands of shares and tens of thousands of shared folders. There are normally thousands of network security groups used to control access to these shares and folders, as well as to mail distribution lists and printers.

Hitachi ID Group Manager is a unique solution, enabling organizations to delegate requests for resource access and authorization for those requests entirely to users, with almost zero setup and no ongoing IT involvement. Users don't need to understand groups – they just browse for shares and

folders. Authorizers need not be manually configured – group owners are automatically tagged as authorizers. Hitachi ID Group Manager eliminates a significant burden of routine change management from security administrators.

- **Secure Kiosk Account**

One of the main challenges in deploying a self-service password reset (SSPR) system, as is found in Hitachi ID Password Manager, is that a significant portion of password problems are at the workstation login prompt. Users forgot their password or triggered a lockout, so can't login, so can't launch a web browser to access the self-service application.

Hitachi ID Password Manager does include client software that extends the login screens to include a password reset button and related elements. A GINA extension service is provided for Windows 2000 and Windows XP (which does not modify the GINA DLL chain). A similar option using the Credential Provider infrastructure is provided for Vista workstations. An IVR solution for telephone password reset is also available.

Most organizations, however, prefer to address the problem of locked out users without deploying client software at all.

Hitachi ID pioneered the security kiosk account (SKA), which enables organizations to create a network user (e.g., called `help` with no password) that can be used to access the SSPR application and nothing else. The SKA uniquely empowers organizations to solve the locked-out-user problem with self-service, without having to resort to a broad deployment of client software.

- **Stateless Single Signon**

Many organizations are interested in reduced or “single” signon for internal users. In practice, this can be difficult to deploy, since E-SSO products, which work by “screen scraping” login prompts on the Windows desktop, must have access to a database of application login IDs and passwords, for every account belonging to every user. Acquiring and maintaining this credential database represents significant cost and security risk, and consequently E-SSO deployments tend to be small in scope.

Hitachi ID's Hitachi ID Login Manager (P-Synch/SSO) product addresses the same functional requirement – reduced signon through screen scraping on the Windows desktop – but without a credential database. Instead, it relies on password synchronization service provided by Hitachi ID Password Manager. Eliminating credential storage (and also scripting) makes Hitachi ID Login Manager uniquely inexpensive to manage, secure and scalable.

17.2 Scalability

Figure 1 on Page 12 highlights differences between the architecture of Hitachi ID Management Suite and other common architectures for identity management systems. Using the optimizations shown in this diagram, Hitachi ID Management Suite is able to process changes, such as auto-discovery of large numbers of users on target systems, 10x to 100x faster than competing products.

In the diagram:

1. The “Optimized” architecture shows the components of Hitachi ID Management Suite. In this diagram:
 - (a) Users access the system using a web browser, connected to a web server using the HTTPS protocol. This is common to all products with a web UI.

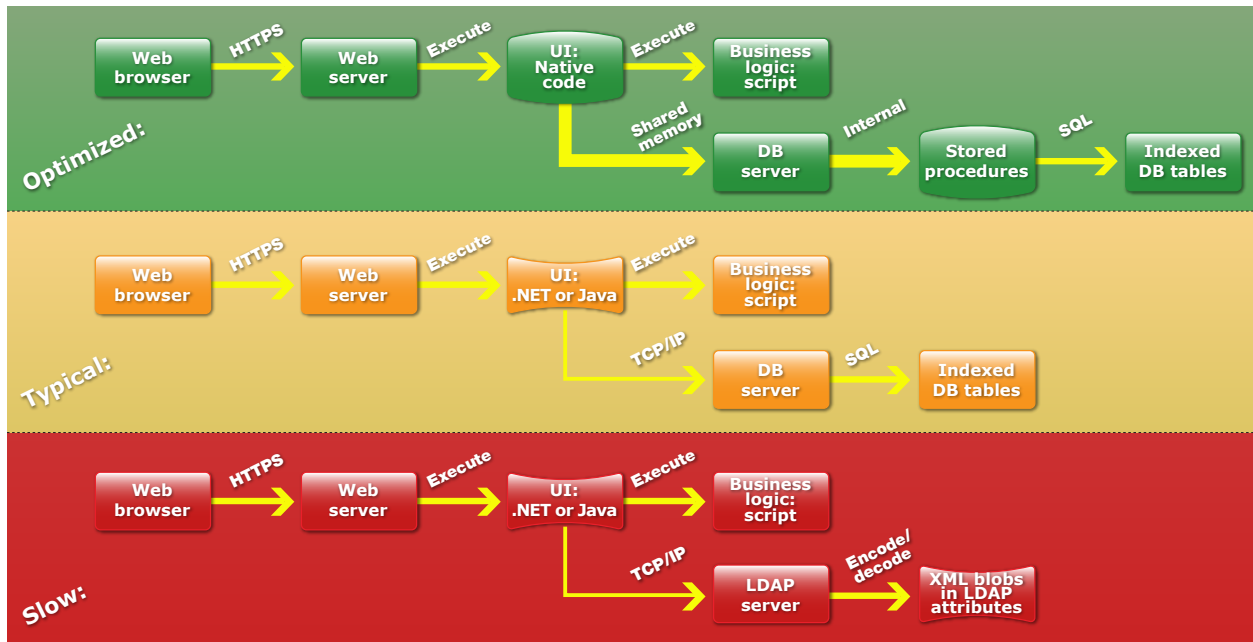


Figure 1: Performance of Alternative IdM Solution Architectures

- (b) Hitachi ID Management Suite’s user interface and core services are implemented using native-compiled IA86 code, which runs very fast.
 - (c) Business logic is added to the system in the form of script code – an approach common to all identity management products and modern products.
 - (d) A database server houses all data: policies, identities, workflow requests, transaction history, etc.
 - (e) Stored procedures act both to isolate the database from the user interface and IdM services and to accelerate the system by performing as much of its processing as possible within the database.
2. The “Typical” architecture shows the components of most competing products. This architecture performs less well than Hitachi ID Management Suite because of the following differences:
 - (a) The UI and IDM services are written in either Java (J2EE) or .NET. Java is typically about 10x slower than native code and .NET is typically about 2x slower than native code.
 - (b) The IdM logic, in both the UI and IDM services, has direct access to the database. Issuing SQL calls directly to the database means that searches and updates that might be accelerated by being run inside the database instead trigger slow network traffic.
 3. The “Slow” architecture shows the components of only one or two competing products. In this architecture, a high performance relational database is replaced with complex XML objects embedded in an LDAP directory. Whenever the IDM system has to look up user profile data or search for users that match some criteria, an XML parser must be applied to each and every user profile. This not only severely impairs performance, but it also makes it impossible to use off-the-shelf tools to write custom reports.

18 How will Version 6.0 of the Hitachi ID Management Suite reduce the need for implementation services?

A number of enhancements in Hitachi ID Management Suite 6.0 support more rapid deployment of the solution:

1. Identity synchronization can now be implemented without writing any code.
 - (a) Profile attributes are defined and mapped to target attributes.
 - (b) Both profile and target attributes are given priority numbers.
 - (c) Flags are set telling Hitachi ID Identity Manager to monitor changes to profile and target attributes.
 - (d) A requester is configured for identity synchronization events.

Once all of the above items are configured – using the web UI – identity synchronization will automatically take place as an integral part of nightly auto-discovery.

2. Auto-provisioning and auto-deactivation is implemented using a new, event-driven model.
 - (a) ID-Compare has been replaced with ID-Track.
 - (b) ID-Track aggregates all detected changes for each user profile and calls a single function, passing in those changes.
 - (c) Customers write business logic that parses detected changes and submits responsive actions to the workflow engine.
 - (d) Example use cases include:
 - i. Detecting changes to personal identity attributes, for example a new phone number in the HR feed, and propagating the new attributes to other login IDs associated with the same user (i.e., identity synchronization as above).
 - ii. Detecting unauthorized changes, such as a user being added to the Administrators group on Active Directory and submitting workflow requests to undo them.
 - iii. Detecting newly created users in a system of record, such as HR, and submitting role-based requests to create login IDs for the same user on other systems and applications.
 - iv. Detecting removal of users from a system of record, such as HR, and submitting "terminate all access" requests to the workflow engine.

3. The workflow API is available directly to business logic.

Customers wishing to develop custom request forms can do so easily, using the development tools of their choice. Forms can submit requests directly to the workflow service over a SOAP API, so that Hitachi ID Identity Manager can track requests through validation, approval and execution.

This API also largely eliminates the need for business logic to perform direct database lookups using tools such as DBCMD.

4. A number of connectors have been enhanced and are more flexible than before.

- (a) The SSH agent has been enhanced and is more easily scriptable.
- (b) A new, XML/web services agent has been added, making it easy to integrate with applications that expose an administrative API over a web service.
- (c) The scriptable database agents have been updated, making them much more flexible and easy to configure.

5. A reference implementation is available on request.

Hitachi ID has developed a reference implementation of Hitachi ID Management Suite, complete with AD and Exchange target systems, validated and authorized request forms and table-driven logic to select OUs, home directory servers and mailbox servers for new users. Customers can examine how this system is put together before beginning their own implementations.