Industry's Only End-to-End Identity Management Solution: Oblix IDLink for BMC

WHITEPAPER

Printed in the United States of America.
Printing Date: July 2002 **Part Number: obx37a**

Oblix, Inc.
18922 Forge Drive
Cupertino, CA 95014, USA
T 408.861.6800 F 408.861.6810

European Headquarters
Regus House, Trinity Court
Wokingham Road, Bracknell
Berkshire RG42 1PL, UK
T +44(0)1344 668 014

www.oblix.com
info@oblix.com

Foreword

Organizations today are extending beyond their traditional boundaries. When that happens, the challenge of establishing effective identification, authentication and access to a variety of systems becomes increasingly complex. This is a familiar problem to all of us in the information technology industry.

PricewaterhouseCoopers has been working with clients all over the world helping to solve the crucial problem of Identity Management. But, as our direct client experience has shown, most of the technologies available today are point solutions, each of which addresses only one of the many components that form a complete Identity Management solution. Our clients are asking us for a simplified process. And as technologies continue to mature, some of the industry's leading vendors are paving the way toward a more simplified approach to Identity Management.

That's why we're pleased to see a newly integrated solution, Oblix IDLink™, from two established leaders in the IT security industry: BMC Software and Oblix. These two vendors have leveraged their individual capabilities and strengths to jointly develop a robust, new enterprise-wide Identity Management solution. The result is something that will help organizations simplify Identity Management across the enterprise – for both end-users and administrators.

Now, as we use our proven methodology to help organizations define and implement integrated Identity Management solutions, we'll be able to offer clients the best of both of these technologies – fully integrated into a solution that provides a single point of access for web and legacy enterprise systems, and one that makes administration simple.

Our clients asked us for help in getting to a more simplified solution. Working together with Oblix and BMC Software, PricewaterhouseCoopers is pleased to offer our clients a new option for enterprise-wide Identity Management. This white paper will explain the details.

– Joe Duffy
Partner-in-charge Security and Privacy Practice
PricewaterhouseCoopers

Oblix IDLink Brings Oblix NetPoint 6 and BMC CONTROL-SA Together for End-to-End Identity Management

The Identity Management Problem

At one time, ensuring that only the appropriate individual or group could gain access to systems and information was relatively easy. For example, when the head of payroll retired after years of dedicated service, his account on the mainframe—perhaps one of the few systems to which he had access—was retired along with him, fairly quickly and easily. Today when the head of payroll retires or leaves the company, he or she may have dozens of accounts on possibly hundreds of different applications and systems, and the process of decommissioning access to all of them can take weeks, as did the process of setting them up in the first place.

As e-business initiatives are woven into the very fabric of the global economy, the problem becomes increasingly complex and costly. Today's enterprise extends well beyond the walls of corporate headquarters, and includes customers, suppliers, and business partners, in addition to employees and contractors, all of whom need varying levels of access to Web-based as well as back-end IT resources. In addition, these relationships and roles are transient at best, with turnover in companies high as people move from company to company—the person who's a dedicated employee one day might be a vendor or a competitor the next.

While the boundaries between customers, partners, and other users have blurred, the boundaries between Web-based systems and traditional IT resources have not: Back-end applications, systems, and resources are often managed completely separately from Web-based systems.

One result is that organizations face an enormous administrative burden as they attempt to provide a seamless user experience to customers, partners, suppliers, and vendors. With each new application that an organization deploys comes another system for creating and managing user accounts and access control that is different from those already used for other applications. Different users may be represented differently across different systems, and information is duplicated, inconsistent, or simply inaccurate, because the manual processes used to configure the various accounts are error prone.

Without automated provisioning companies suffer a combination of reduced productivity, satisfaction, and revenue exacerbated depending on the time if takes to create accounts and deliver access to applications or services. User productivity suffers when

new employees or consultants cannot access the applications that they need to do their jobs because their accounts are waiting to be created in the systems and applications they need. And the revenue stream and satisfaction is reduced when partners and suppliers can't take advantage of new e-business applications because their accounts haven't been created. In the information age, people have developed a demand that requires companies to be able to deliver near real time access to the systems or services that they need. For companies delivering services, often there is no second chance with a consumer, once users sign up, the service should be able to be delivered immediately. Online enrollment, which was once considered a convenience, is now a business necessity. Employees also demand the same level of service that they are used to from other online businesses.

The Integrated Solution: Oblix IDLink

These are the types of problems solved by Oblix IDLink™ . Oblix IDLink integrates identity management, provisioning, and access control. Developed by Oblix Inc. in cooperation with BMC Software, Oblix IDLink facilitates end-to-end identity utilization between Oblix NetPoint and CONTROL-SA from BMC Software, bringing together the best features of two best-of-breed solutions to provide end-to-end identity management.

By using Oblix IDLink with Oblix NetPoint and CONTROL-SA, organizations can leverage the key strengths of both products to ensure common, consistent identity management for both intranet and extranet users and their access privileges across multiple systems and applications. Before delving into the specifics of Oblix IDLink, let's take a closer look at some of the features provided by these two products.

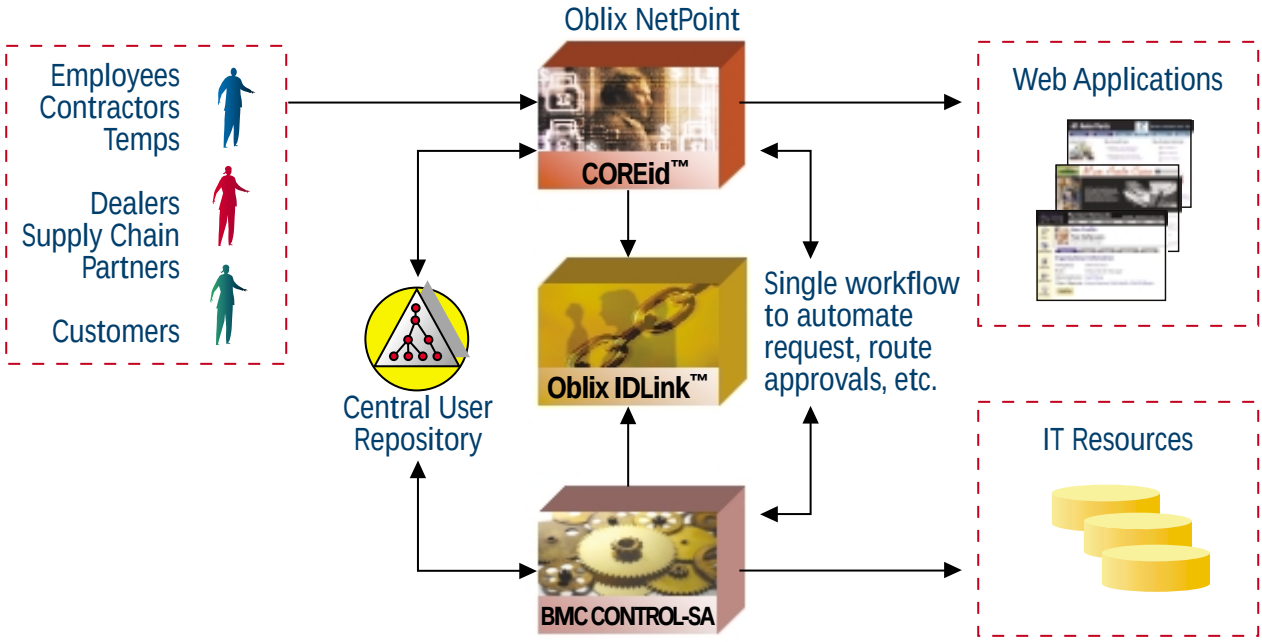

Figure 1: Oblix IDLink - Uniting Two Best-of-Breed Solutions

Oblix NetPoint for Web Access and Enterprise Identity Management

Oblix NetPoint provides Web access management and enterprise identity management. Oblix NetPoint comprises two powerful systems that leverage the concept of a digital identity — an object that represents a user — stored in an LDAP directory:

- NetPoint Access System delivers common security across multiple Web and non-Web servers and applications to ensure that only authorized users can gain access to information, applications and resources residing across virtual organiztions. Oblix NetPoint Access System provides strict, standards-based authentication and authorization, Web single sign-on, and common resource security across multiple servers.

- NetPoint COREid™ System puts digital identity at the center of an e-business environment. It manages user identity, group membership, and organization information and access privileges across all Web applications. Powerful self-service features, multi-step customizable workflow processes, IdentityXML and delegated administration capability ensure that user identity information is continually kept current, even in dynamic e-business environments and across partner organizations.

For example, a manufacturer provides access to an order-entry system and customer care to its partners via its corporate Web site. Rather than creating the necessary 10,000 user accounts for its partner's employees directly, the manufacturer has delegated this responsibility to its twenty-five partners by creating just a handful of accounts for partner administrators. These administrators have access to a select subset of applications and privileges, and can effectively shoulder the burden of creating and managing those users inside their own companies who are entitled to access the applications.

The first time a new user from a partner-company tries to place an order at the site, he or she completes a form, creating a user name and password, and provides other details. Submitting the form over the Website initiates a workflow that sends the request for a new account to the partner-administrator at the partner company. The partner-administrator approves the request or rejects it. If the request is approved, the next time the user logs in at the manufacturer's Website, a Web server plug-in (WebGate) intercepts the partner's logon credential and sends to the Oblix NetPoint Access System, which authenticates the user and provides access to those systems for which the user is authorized. The user can access the Web-based order-entry system, and can register for new applications as they become available.

With Oblix NetPoint providing the company's security infrastructure, the benefits don't stop with any single implementation. Because access privileges are tied to the digital identity, the applications and resources that can be exposed to any customer, partner,

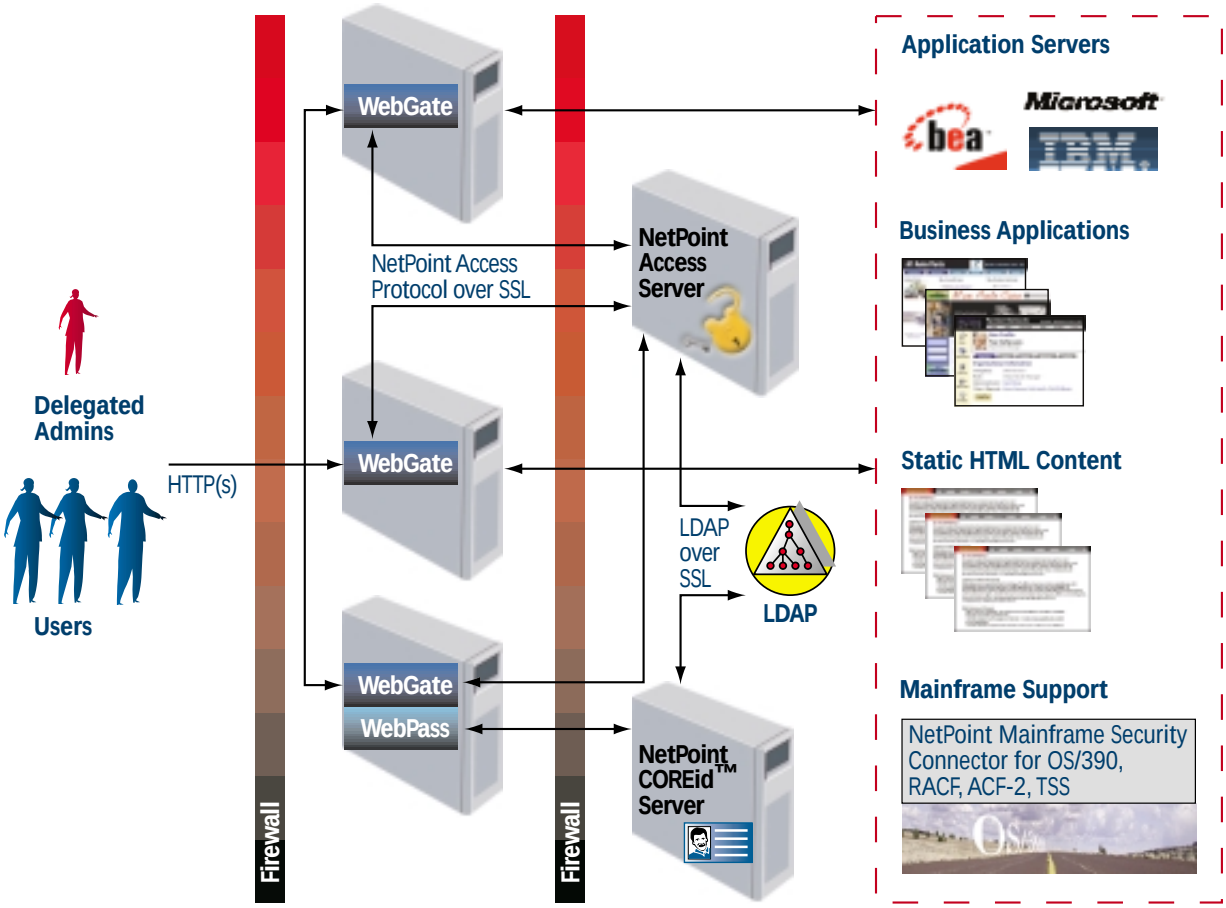

Figure 2: Oblix NetPoint Architecture

or employee can also be completely customized at a very granular level, based on any attribute (or number of attributes) associated with any digital identity. So, after six months of successfully supporting the direct order-entry system for its partners, when the manufacturer implements a new customer care system that distinguishes between partners based on gross sales (using an attribute called "partner level" with possible values being "silver," "bronze," and "gold"), a partner still logs on only once and gains immediate access to this new system automatically. In addition, the user's view of the manufacturer's portal site is completely customized, based on the attributes embedded in the digital identity. For example, "silver" partners see one price list; "gold" partners see another.

CONTROL-SA from BMC Software and Enterprise User Provisioning

CONTROL-SA is the world's most robust enterprise user provisioning solution. Provisioning is an automated process that encompasses all the steps required to manage — setup, change, and disable — user or system access and entitlement rights to applications, servers, and network services. CONTROL-SA stores all provisioning logic needed to connect the right people to the right resources in the organization. It provides a central point of control to back-end heterogeneous IT resources and enables security administrators to easily manage users, access to resources, and security policies.

CONTROL-SA comprises a central enterprise security server, the Enterprise Security Station (ESS), and Agents that run on the various target platforms and applications — including mainframes , midrange servers, Windows, directories, databases, email systems, HR, CRM, ERP, and other back-end systems. The ESS repository functions as the system's central repository, storing security information of managed systems. The agents provide the interface between CONTROL-SA and the native security environments of each controlled system (the Resident Security System, or RSS). CONTROL-SA supports over 50 RSS types with SA-Agents (shown in Figure 3). CONTROL-SA also provides an open architecture for configuring more SA-Agents and further extending the available RSS coverage.

CONTROL-SA offers additional functionality that increases its comprehensiveness and effectiveness. For one, CONTROL-SA provides complete auditing of enterprise-wide security modifications. Its advanced policy-based management enforces unified standards and policies for all managed systems. Furthermore, it offers various password management capabilities such as password synchronization and challenge/response login.

CONTROL-SA provisions user accounts on multiple target systems based on the configuration of an "Enterprise User," a global user account internal to CONTROL-SA that relates to all other user accounts on target systems. Associated with each Enterprise User is one or more Job-Codes. "Job-Codes" are a feature within BMC CONTROL-SA that logically binds a defined role (Job-Code) with system resources that are required for a user to perform that job function. A user can have multiple Job-Codes assigned, and a Job-Code can have multiple back-end IT resources assigned. These Job-Codes are defined with BMC CONTROL-SA and are a key component in driving the provisioning process within BMC.

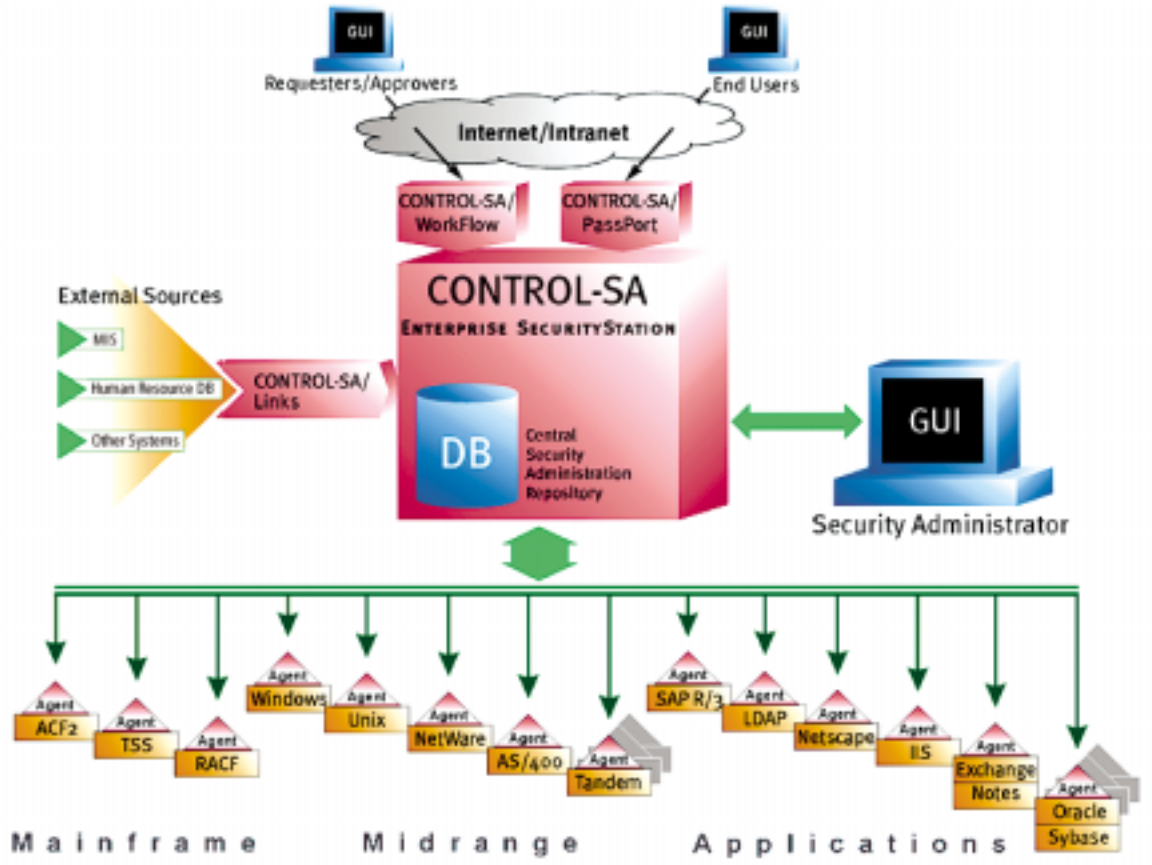

Figure 3: CONTROL-SA Architecture

For example, a "basicemployee" Job-Code might encompass a Windows NT domain logon, an account on a Solaris host, and an account on the Exchange mail server; basicemployee might be the only Job-Code associated with the enterprise user account of an entry-level accounting clerk. When the clerk is promoted to senior staff accountant, he or she acquires an additional Job-Code, "finance," which has privileges on Oracle Financials and several other back-end systems. When a Job-Code is removed from an enterprise user, the user loses the privileges that were associated with the Job-Code. When employees leave an organization, their Job-Codes are removed and enterprise user accounts, along with all associated access privileges, are revoked automatically and optionally deleted.

The ESS server keeps track of all this information, updating its database with the new information and passing a create/update/delete commands to the SA-Agent, which in turn passes the information via an API call to the RSS of each of the specific platforms. Each target system's RSS then executes the commands on the target system for the Enterprise User.

Oblix IDLink: End-to-End Integrated Web Access, Identity Management, and Enterprise User Provisioning

With Oblix IDLink, both Web and e-business resources and traditional IT resources—payroll systems, HR systems, CRM, and ERP—can leverage the digital identity to drive user provisioning across all systems using sophisticated workflows that automate process and ensure coherent, consistent, policy-based security administration.

The Oblix IDLink provides:

- Single point of control through the NetPoint COREid GUI for managing digital identities and access rights for all users to all applications throughout the extended enterprise;
- Single process for end-to-end user set-up, user changes, and de-activation of user accounts in both Web-based and back-end IT resources;
- Single workflow system that automates requests and approvals for new users and their access to both Web based applications and back-end IT resources;
- End-to-end self-service and self-registration through one interface for all applications;
- End-to-end delegated administration enabling the administering of both provision ing users to IT resources and user identity management to be distributed through out the extended enterprise.

Oblix IDLink enables Oblix NetPoint and CONTROL-SA to combine forces to effectively manage access privileges across multiple, both Web-based and traditional IT systems. It combines role-based (access to applications based on a single attribute) and rule-based (access to applications based on a combination of roles or a specific business rule) provisioning and identity management, providing maximum flexibility in developing access rights for complex environments. Oblix IDLink for BMC comprises two key software components, both of which reside on the NetPoint COREid Server:

- The Oblix IDLink Provisioning Module extends the functionality of the Oblix NetPoint COREid system as the foundation for driving provisioning through CONTROL-SA from BMC. The IDLink Provisioning Module provides the capability to create, manage workflows and apply rules that determine which users have access to specific Job Codes for provisioning. The NetPoint COREid workflow has been enhanced to spawn the multiple subflows required for approvals by individual resource owners. The Oblix IDLink Provisioning Module comprises the ability to apply logic to the provisioning process through Job-Codes, machine names, machine types, user groups, approvals, rules engine, and web based GUI user interface for creation and management of workflow and sub-flows.

- The Oblix IDLink Provisioning Bridge enables CONTROL-SA Job-Codes, synchronized in Oblix NetPoint. The Oblix IDLink Provisioning Bridge also supports error handling and messages such as confirmation of provisioning

events from CONTROL-SA. The Oblix IDLink Provisioning Bridge ensures that duplicate entries are not created and checks confirmation and other error messages to will ensure that provisioning actions have been successful. When faults are found the IDLink Provisioning Bridge reports status back to the NetPoint administrator.

The Oblix IDLink solution enables organizations to fully automate the process of creating users, deleting users, and managing the changes to user identity throughout the entire enterprise. The Oblix NetPoint workflows play an important part in each of the tasks, essentially driving the process.

Synchronizing BMC Job-Codes in Oblix NetPoint

During Oblix NetPoint system installation and configuration, Oblix IDLink is configured to manage Job-Code objects in the central LDAP directory. The Job-Codes themselves are modeled in the LDAP hierarchy as an object class that includes attributes such as machine name, machine type, Job-Code name, and approval flags. The approval flags are an Oblix-added feature designed and required to support the workflow.

In addition, Oblix NetPoint user objects are extended with two new attributes: a multi-value attribute for Job-Code, and an attribute for the CONTROL-SA Enterprise User ID. Once the Job-Code object has been created in the LDAP directory, the Oblix IDLink Provisioning Bridge automatically connects with the CONTROL-SA Job-Code subsystem and synchronizes the information in the Job-Code class (in Oblix NetPoint's LDAP directory) with the data in CONTROL-SA. The Job-Codes become available on the Oblix NetPoint user interface via a drop-down list; the specific Job-Codes in the list will vary dynamically, depending upon the privileges and role of the administrative user logged on to the system.

After Oblix IDLink is installed, Job-Codes will continue to be created and managed in CONTROL-SA; the ESS Server contains provisioning logic, Job-Codes mapping, account-creation templates, and settings for each CONTROL-SA Agent implemented and how it interacts with its respective RSS. The BMC ESS graphical user-interface is used to define and administer these entities in the ESS Server. Job-Code information is synchronized automatically between CONTROL-SA and Oblix NetPoint, at configurable intervals, or, immediately, when changes are made, by using Identity XML (in Oblix NetPoint) or direct update of LDAP.

One of the features of Oblix IDLink is the delivery of both rules- and role-based provisioning. Filter-based rules allow administrators to selectively show certain Job-Codes depending on existing values in NetPoint User Manager and Organization Manager. Plus, these rules can be both static and dynamic. Dynamic rules allow administrators to select Job-Codes on the fly, based on the current user's profile. Additional attributes can be added to the Job-Code mapping object that allows for more complex rules to be defined.

Once the Job-Codes exist in the Oblix NetPoint LDAP directory, administrators must configure and customize the various workflows that will drive provisioning, and the workflow component of Oblix NetPoint is the primary interface for doing so.

Oblix NetPoint Workflow Drives the Provisioning Process

The Oblix IDLink Provisioning Module extends the Oblix NetPoint administration GUI to support the provisioning workflow capabilities. The Oblix NetPoint GUI is used to configure all workflows to create new users, delete users when necessary, and modify user account information. Workflows can contain sub-workflows, and workflows can be based on change-attributes that trigger events throughout the system when such events occur—a change in job title or status with a partner company, for example. Using the Oblix NetPoint GUI, an administrator can define an integrated Create User workflow that identifies the CONTROL-SA Job-Codes, machines, and approvals that are necessary to provision the user. The workflow would include a step or steps that essentially embeds calls the CONTROL-SA ESS Client Interface. The external step can comprise as many sub-steps and approvals as are necessary to accurately create, delete, or modify a user. Delegated administrators can be included in the approval process.

For example, a large aerospace company wants to provide access for all senior sales staff—some 450 people—in the Asia-Pacific region to access a new Siebel 7.0 sales system. A workflow has been defined to support self-registration and automated access, and the workflow can be initiated by entering information in a customized form is available on the extranet Web site.

When a salesperson from Asia-Pacific submits the form, a workflow based on the user 's profile information is initiated that contains the correct BMC Job-Code information for that user. The workflow will create the user and assign the user to the appropriate group that has access to the Siebel application. The Job-Codes associated with the user's role will be provided to CONTROL-SA to initiate creating the account on the back-end systems, as defined in the Job-Code. Approvals based on the user and workflow enable the account to be created in Siebel. Once the account is created, access is controlled based on this user's group membership or attribute value.

Following is the process flow for self-registration and automated account creation in back – end systems through CONTROL-SA:

- A "Create User" workflow is configured in the NetPoint Workflow GUI by an administrator. The workflow defines the BMC Job-Codes, machines, approvals, and participants necessary to approve and execute the provisioning actions.
- Creation of the workflow is dependent on the synchronization of the Job-Codes with NetPoint COREid. The Job-Codes are exposed in the NetPoint workflow GUI based on the identity of the logged in user. This allows administrators only with the proper access privileges to define provisioning workflows for the selected systems.

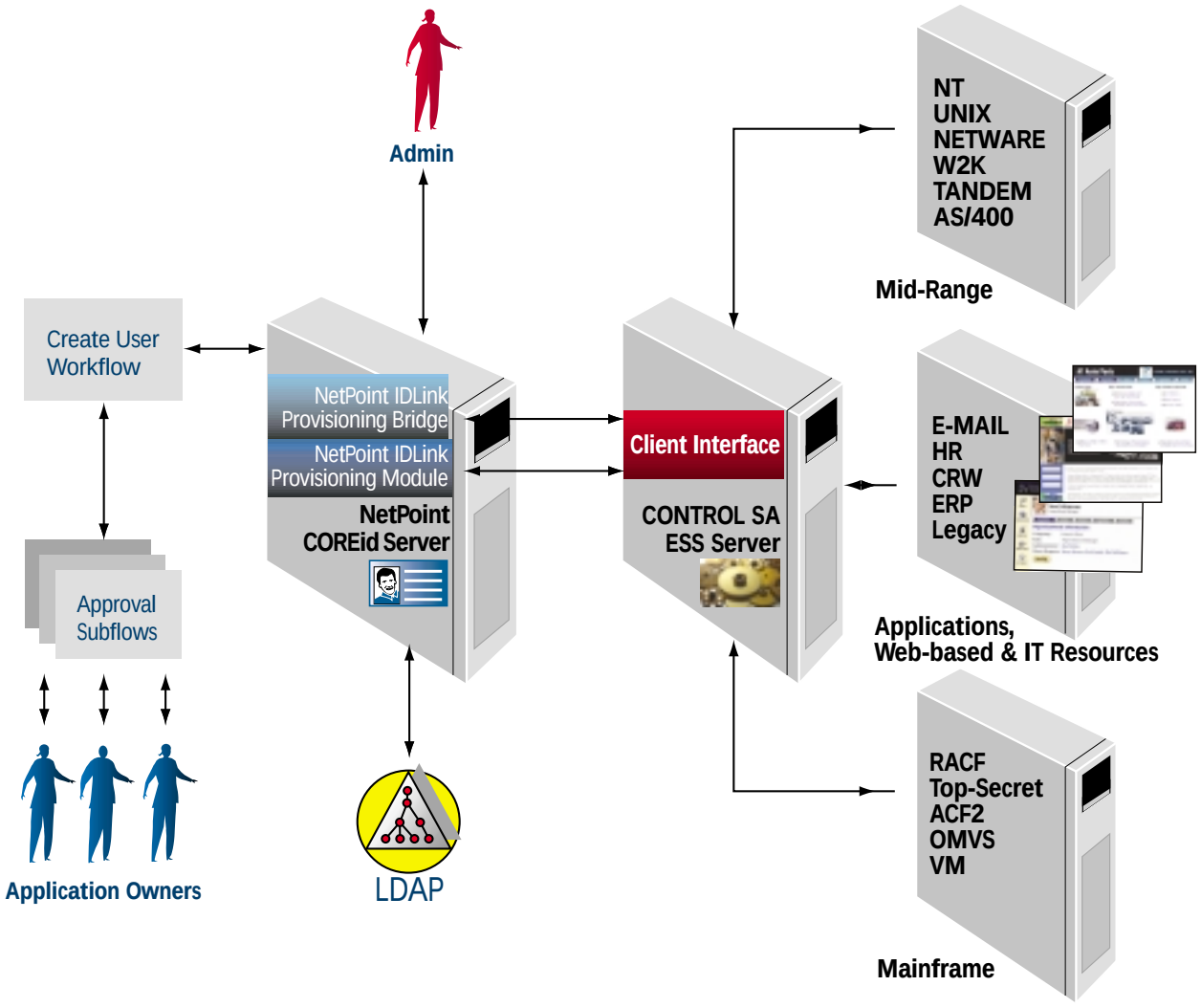

Figure 4: Process Flow for Adding a New User

- An end user self registers using a web-based form. This initiates a workflow that routes tickets to the participants as configured for approvals. Once all participants provide their approvals, Oblix IDLink initiates the provisioning actions through CONTROL-SA.
- The IDLink Provisioning Bridge communicates with the CONTROL-SA ESS Client Interface. The IDLink Provisioning Bridge calls the ESS Server to ensure that a duplicate entry is not created in the ESS database. If the ESS Server responds with an error message, the workflow will terminate and send a message to the NetPoint administrator.
- If the user does not yet exist, the Oblix IDLink Provisioning Module routes the workflow tickets, with approval information, for each of the accounts associated with the role defined by the Job-Code.
- Once the Oblix NetPoint workflow tickets are approved, Oblix NetPoint issues an external call to CONTROL-SA.

- CONTROL-SA receives the commands and Job-Codes necessary to perform the actions required—create, delete, or modify—and returns the confirmation information. Specifically, the BMC ESS Server processes the call (request) from Oblix NetPoint, and passes the processed request to the SA-Agent.
- The SA-Agent interfaces with the ESS and issues commands to create, delete, or modify accounts.
- Oblix NetPoint receives a return code confirming or negating the completed provisioning, de-commissioning, or modification actions.

The integrated create user workflow proceeds only if all the approval subflows are successful. If any approver along the way rejects any portion of the process or a sub-process, the workflow generates an error message, the workflow stops, and no accounts are provisioned, nor are any other changes made until action is taken on the error message.

All provisioning logic resides in CONTROL-SA. Once the user is provisioned, the success or failure of the account setup is sent to Oblix NetPoint. Oblix NetPoint executes proper error handling upon failure, or commits the user and completes the workflow event.

Because Oblix NetPoint triggers the provisioning process, provisioning events can be based on any user attribute of the digital identity. The integration with CONTROL-SA enables an Oblix NetPoint identity to support a BMC Job-Code as an attribute. For example, an accounting promotion to senior staff accountant can trigger a "change-attribute" workflow associated with the Job-Code attribute of the user's digital identity, initiating a workflow ticket for approval to senior management. Once the senior manager approves the workflow ticket, subsequent workflows associated with this change then provision the appropriate accounts on the back-end IT resources required to completely enable the senior staff accountant.

But because the organization also has Oblix NetPoint, this employee can take advantage of single sign-on to all internal Web-based applications. He or she can also self-enroll for new applications using the web site, and he is automatically enrolled in new applications when they become available.

Summary

Managing user accounts and ensuring that only the appropriate people can gain access to important resources is challenging even in the smallest of organizations. When the enterprise resources number in the hundreds or thousands, and when the numbers of users that need to be provided (or prevented from having) access number in potentially the millions, the task is daunting. E-business initiatives will succeed or fail as the costs associated with implementing them are measured against the return on investment; if the costs include a swat team of administrators dedicated to handling user provisioning across a proliferation of disparate Web-based and heterogeneous back-end IT systems, any real savings is substantially diluted.

With Oblix IDLink, both Web and e-business resources and traditional IT resources — payroll systems, HR systems, CRM, and ERP—can leverage the digital identity to drive user provisioning across all systems using sophisticated workflows that automate the process and ensure coherent, consistent, policy-based security administration.

The Oblix IDLink solution is unique: there's nothing else like it on the market today. Without it, you can provision and control user identity on Web-based applications — but you cannot automatically create matching user accounts on the mainframe, UNIX, mail system, SAP, Siebel, and other heterogeneous IT systems and applications in your environment.

Without it, you have a proliferation of user accounts that must be managed by an army of administrators, and frustrated users—employees, business partners, customers — who can't purchase your products or services, or get their jobs done. Without it, you have redundant user accounts and conflicting security policies, rather than a single digital identity that can be used across multiple systems.

Oblix IDLink combines role-based provisioning and rule-based identity management, providing maximum flexibility for managing access rights in complex environments. Your organization can provide access to IT applications based on a single attribute of the digital identity, and provide access to Web-based applications based on a combination of roles or a specific business rule. The result is a flexible identity management infrastructure that provides unlimited opportunity to leverage existing applications and implement new e-business initiatives, ultimately improving competitive position.