zapthink white paper

THE CRITICAL NEED FOR ENTITLEMENT MANAGEMENT IN SOA

FINE-GRAINED AUTHORIZATION IN THE CONTEXT OF SERVICES

ZapThink, LLC • 108 Woodlawn Road • Baltimore, MD 21210 • info@zapthink.com • www.zapthink.com

THE CRITICAL NEED FOR ENTITLEMENT MANAGEMENT IN SOA

FINE-GRAINED AUTHORIZATION IN THE CONTEXT OF SERVICES

March 2007

Analyst: Jason Bloomberg

Abstract

Entitlements are the corporate, industry and contractual rules that determine access privileges to resources for a specific individuals, groups of individuals, applications, or even Services. *Entitlement Management* is the administration, enforcement, auditing, and review of policies for determining whether a particular entity is entitled to take a particular action or access a particular bit of information, given the context of the request. Because entitlements are a form of policy, Entitlement Management is a form of policy management, which is an integral part of SOA governance for those organizations who are implementing Service-Oriented Architecture (SOA).

Securent's Entitlement Management Solution provides scalable, flexible Entitlement Management functionality that extracts and loosely couples access control from underlying individual applications, providing policy enforcement at a finer level of granularity, and with greater precision, than any Web Single Sign-On approach to access management. Furthermore, since Securent exposes its Entitlement Management capabilities as standards-based Services, any organization implementing SOA can include Securent's capabilities as an integral part of their SOA rollout.

All Contents Copyright © 2007 ZapThink, LLC. All rights reserved. The information contained herein has been obtained from sources believed to be reliable. ZapThink disclaims all warranties as to the accuracy, completeness or adequacy of such information. ZapThink shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice. All trademarks, service marks, and trade names are trademarked by their respective owners and ZapThink makes no claims to these names.

I. SOA and the Problem of Authorization

Service-Oriented Architecture (SOA) is an approach to organizing IT resources to meet the changing needs of the business in a flexible, dynamic manner. At the core of SOA is the *Service abstraction*, which represents heterogeneous software functionality and data as loosely coupled, composable, and discoverable Services. While implementing SOA properly is not trivial, many organizations have successfully implemented the architecture and necessary infrastructure to build and support a Service abstraction that is able to provide the agility benefits that SOA promises to the business.

Among the challenges organizations face as they seek to implement SOA is the problem of the security context for Services. By their nature, Services abstract users from the applications underlying the Service abstraction, but in so doing, Services also disconnect those users from the security context for those underlying applications, for example, when a Service abstracts capabilities from two legacy applications that each handle authorizations in a different way. For this reason ZapThink refers to security as the first roadblock to SOA adoption, because without a way to maintain the security context of users across the Service abstraction, no organization will be able to compose arbitrary Services, and thus realize one of the main benefits of their SOA implementations.

Security is the first roadblock to SOA adoption.

One key to removing this roadblock to SOA adoption is to deal with the problem of authorization. *Authorization* is the act of determining whether a user (or system, process, or Service) is or is not allowed to perform some operation or view some data. There are two broad categories of authorization:

- *Coarse-grained entitlements* – high-level access control decisions that apply to an entire application, Web site, or Service, yet are also typically devoid of application or Service-specific context.
- *Fine-grained entitlements* – finer level access control decisions, including access to objects or functions within applications, parts of Web pages, elements in XML documents, or records in databases.

Entitlements are the corporate, industry and contractual rules that determine access privileges to resources for a specific individual or group of individuals.

Entitlements, then, are the corporate, industry and contractual rules that determine access privileges to resources for a specific individual or group of individuals. Supporting coarse-grained entitlements offers one line of defense for securing Services, but is inadequate for all but the most rudimentary purposes--essentially an all or nothing approach. On the other hand, the need for fine-grained entitlements has been around for a long time, but in general, individual applications handled such entitlements in separate, proprietary ways, typically involving custom coding. As a result, many organizations have been looking to provide authorization as shared infrastructure that many applications can leverage as opposed to such one-off, application specific implementations.

With the rise of SOA, the need to support fine-grained entitlements in an application-neutral fashion that users can easily share within and across composite Services that abstract a wide variety of heterogeneous applications has become both urgent and mandatory. To fully understand this need, it's important to review traditional approaches to Entitlement

Copyright © 2007, ZapThink, LLC

Management, and then discuss how best to tackle Entitlement Management in the context of SOA.

Entitlement management is the administration, enforcement, auditing, and review of policies for determining whether a particular individual or role is entitled to take a particular action or access a particular bit of information, given the context of the request.

Why Traditional Approaches to Entitlement Management Fall Short

Entitlement management is the administration, enforcement, auditing, and review of policies for determining whether a particular individual or role is entitled to take a particular action or access a particular bit of information, given the context of the request. Traditionally, organizations managed entitlements on a siloed, application-by-application basis, or in the context of the Web, via password-protected areas of Web sites. While such approaches are clearly better than no security at all, they suffer from several serious shortcomings:

- Such access control-based Entitlement Management is an "all or nothing" affair: once a user has access to an application or a Web site, they have access to everything, presenting a challenge for companies that must represent complex business relationships or expose the same application to different customers or partners.
- Generally, each application and Web site has its own mechanism for handling both authentication and authorization, leading to complexity and difficulties with management, control, and visibility.

Traditional approaches to Entitlement Management fall into three basic areas: application-specific solutions, Web SSO-based techniques, and billing engine-based Service Provider approaches. These approaches as well as their drawbacks appear below.

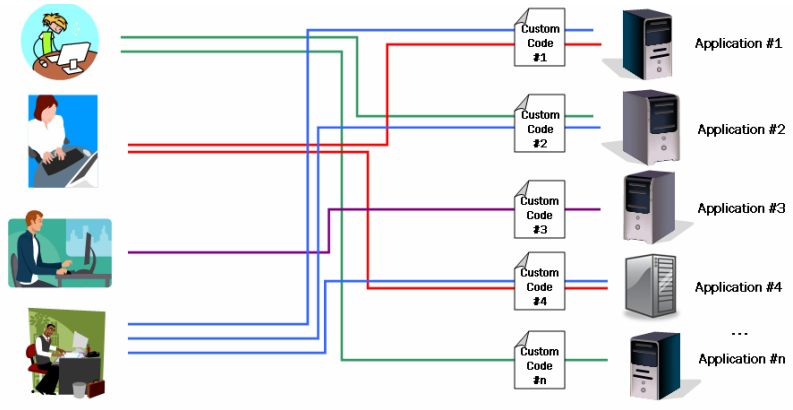
The Application-Specific Solution

First, consider application-specific access solutions. Such solutions control access to a particular application, the transactions it performs, and the data it accesses. Application-specific access approaches typically involve hard-coded entitlement rules. For example, a system might determine that a particular level of manager can approve an order without comparing the order amount to the spending limit. As a result, as business requirements evolve, it is up to the IT department either to reprogram the application (when feasible, which is uncommon), to modify the database or directory, or to create a custom wrapper for the application that can interpret the new business rules.

As the number of such applications grows, and the complexity of changing entitlement requirements also increases, the application-specific approach becomes inflexible to changes in business conditions, costly to maintain, difficult to audit, and its performance also suffers from its inherent complexity. An illustration of the application-specific access control approach appears in the figure on the next page.

Copyright © 2007, ZapThink, LLC

Application-Specific Access Control Solution



Source: ZapThink

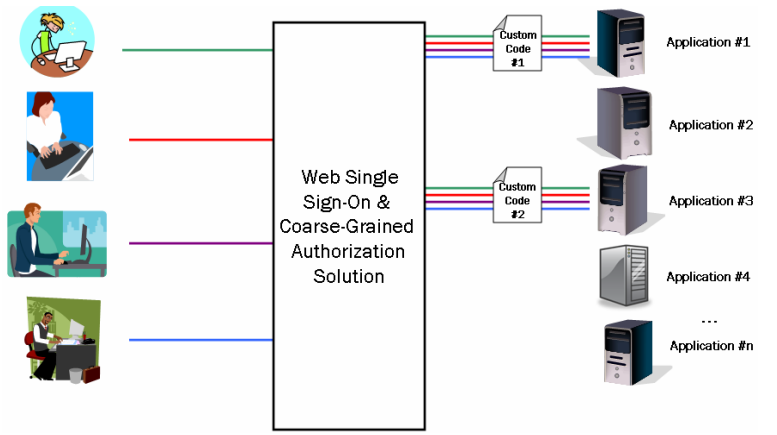
In the application-specific access control solution above, the creator of the application and the IT staff hard-code the entitlement logic, the business rules, the relationships, as well as the linkages.

The Web Single Sign-On Solution

Many organizations who have been struggling with application silos and their application-specific access control approaches have invested in Web single sign-on (SSO) projects in order to provide a single user context for authentication and authorization across multiple applications. Web SSO solutions work by creating a single identity token, and then interchanging it with multiple authentication systems. In essence, the Web SSO system serves as an identity proxy that utilizes a central directory as a way of centralizing identity and access control.

In many cases, the implementation of a Web-based portal or public Web site has been the critical impetus for these Web SSO initiatives, because such interfaces consolidate access to various applications, exposing the need to have a single username/password pair for each user. A Web SSO system is illustrated in the figure below:

Web Single Sign-on System



Source: ZapThink

Copyright © 2007, ZapThink, LLC

Web SSO solutions have their drawbacks, however. They generally do not deal well with legacy applications that lack a Web interface (hence the applications with no connections in the figure above), and they leave critical access policies and access related logic in the applications. Web SSO solutions cannot take the application context into account because application-specific context is close to the application, but typically not available at a central point. As a result, they are more appropriate for coarse-grained entitlement decisions.

Furthermore, Web SSO systems generally don't extend the inherent access rules and entitlement policies that belong to the Web and legacy application. In such cases, Web SSO systems basically act as an agent for the user. These systems store the user's password in a protected database or directory in order to send the password to the legacy application upon login to initiate access. At that point, the Web SSO solution passes control to the legacy application. As a result, Web SSO systems have limited facilities to insert themselves into the flow of the applications, limiting their ability to make real-time decisions on fine grained entitlement rules like time-of-day requests without extensive, inflexible custom coding.

In the context of SOA, the simplistic all-or-nothing security that Web SSO provides is woefully inadequate to secure all the functionality a business Service might provide.

In the context of SOA, the simplistic all-or-nothing security that Web SSO provides is woefully inadequate to secure all the functionality a business Service might provide, because business Services might provide a broad range of data or functionality to a particular consumer. Similarly, application-specific security cannot address the entitlement requirements of loosely coupled Services either, because those Services may abstract functionality from multiple applications. Furthermore, hard-coded security logic in a Service leads to a loss of the loose coupling that is a fundamental tenet of SOA. The bottom line is that SOA requires Entitlement Management for effective security.

The Service Provider Approach

While the SSO approach in the previous section applies to many enterprises, an increasing number of firms seek to offer various types of Services to their customers, combining Web access, Web Services capabilities, as well as Software-as-a-Service (SaaS) offerings. Such Service Providers include telecommunications carriers, an increasing number of third-party Service Providers that offer specialized Services on behalf of enterprise customers, as well as enterprises that build internal Service Provider capabilities.

Many of these Service Providers traditionally perform various Entitlement Management functions through their metering or billing systems, because such systems authorize and track each customer's Service usage, and thus require a point of authentication and authorization for individual users. Such legacy billing systems play a vital role within each Service Provider's infrastructure, acting as the starting point for centralizing Entitlement Management. These billing systems access large amounts of data and typically have high scalability and fault tolerance.

Service Providers often leverage multiple billing systems to manage and bill for different Services or customers. In this approach, a separate connection to a single billing system handles each Service separately. The billing systems have difficulty exchanging customer information with each other, leading to an inflexible siloed organization that negatively impacts

Copyright © 2007, ZapThink, LLC

the customer experience, and furthermore, customers have no real visibility or control of the entitlements, making audits difficult.

Service Providers are now realizing that while billing systems can provide a basic level of entitlement support, such systems also present many challenges to the organization. In particular, the traditional approach requires complex integration among disparate billing solutions, leading to high costs and problems with limited flexibility. Such Service Providers also find it difficult to properly analyze data from the various billing systems in order to make critical business decisions. Furthermore, the problem remains that Service Providers must still write custom code to manage, enforce, and audit entitlements for each Service they provide. Customers want to control who can access the Service they are outsourcing. Either the customer or the Service Provider implements the access logic, and exposes that logic as a Service that the customer can configure.

II. Entitlement Management as an Enabler for SOA

Rather than simply inserting another authorization component in the infrastructure, organizations require a more flexible way of organizing their existing application resources to provide increased flexibility. In other words, organizations require better *architecture*—in particular, an architecture oriented toward the Services that represent that application functionality to the user. *Service-Oriented Architecture* (SOA) is such a set of architectural best practices that enable organizations to leverage resources as flexible Services that the business can leverage dynamically to meet changing business needs.

Service-Oriented Architecture is a set of architectural best practices that enable organizations to leverage resources as flexible Services that the business can leverage dynamically to meet changing business needs.

The rise of SOA in today's enterprise, however, brings with it new challenges, including the first roadblock to SOA adoption: security. While threat management is critical to the success of any SOA initiative to be sure, and because security is such a critical roadblock to successful SOA adoption, architects must resolve the Entitlement Management problem to get the flexibility they need. Understanding the relationship between Entitlement Management and SOA, therefore, is a critically important part of achieving success with either initiative.

The Rise of Enterprise Entitlement Management Systems

Enterprise Entitlement Management systems are a relatively new category of software that dynamically manages real-time access to applications, transactions and data within enterprise-scale computing environments. Fundamentally, Entitlement Management provides an abstracted security layer that enables IT departments to create or deploy applications that improve the user experience consistently across any customer touchpoint. Entitlement Management systems handle any type of application, and extract all entitlement rules into a policy database they can apply specifically to an application and consistently across all applications.

In fact, even if there is only one application or Service, externalizing the entitlements through an Entitlement Management system supports declarative, dynamic policy changes and enables the external review and auditing of the policies. Entitlement Management systems thus provide both fine-grained transactional entitlements, collaborative entitlements, as well as coarse-grained entitlements.

Copyright © 2007, ZapThink, LLC

Entitlement Management systems provide a single point of control for making dynamic access control decisions.

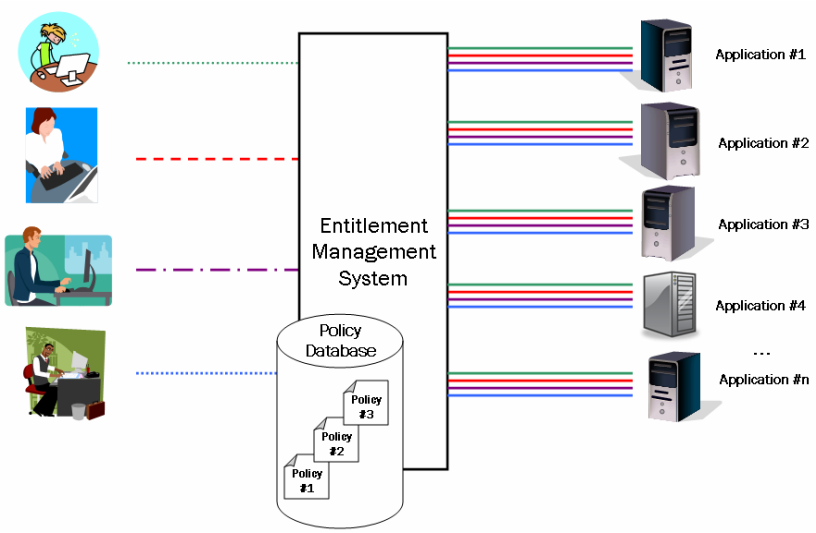
Transactional entitlement Services sit between Services and the applications they expose and verify transaction requests for those applications at runtime. *Collaborative entitlement* allows multiple applications to share data and transactions as part of an access decision process. Relevant resources that are otherwise outside the application flow can affect the entitlement decision.

Entitlement Management systems provide a single point of control for making dynamic access control decisions based on any number of independent criteria, by leveraging the following capabilities:

- Externalization of access control and related entitlement policies from the applications they support to increase the manageability of those policies and to enable real-time access decisions.
- Passing of access decision requests to other applications based on fine-grained access control policies, enabling the construction of richer, dynamic entitlement decisions, for example, establishing limits on specific transactions.
- Support for distributed, transactional architectures that must handle numerous Services and large volumes of access criteria without inhibiting the performance of the operational system.

An illustration of an Enterprise Entitlement Management System appears in the figure on the next page:

Enterprise Entitlement Management System



Source: ZapThink

Entitlement Management systems externalize entitlement rules into a policy database and then apply them across all applications, providing fine-grained, real-time access control for data and applications across all customer touchpoints. The figure above illustrates the fine-grained nature of the access via the different dashed lines connecting the users; each one is entitled to access different data or functionality from each of the various available applications. These systems thus address SSO's drawback of its reliance on coarse-grained, all-or-nothing entitlements.

Copyright © 2007, ZapThink, LLC

Entitlement Management also addresses Service Providers' challenges with siloed billing systems by providing centralized access to information and gathering and storing user data from multiple databases within each billing system. By serving as a central repository of policies, the Entitlement Management system simplifies business intelligence and compliance audit data gathering efforts, and helps to create a more complete view of each customer across various lines of business.

For Service Providers, Entitlement Management systems provide more value than simply determining which customers can access which content. Within the context of the Service instance for a given customer, the systems can delegate to the customer the ability to specify the entitlement policy, allowing the Service to adhere to the customer's security and compliance model. Such systems can also enable a variety of new converged Services through greater control and variability of matching customer desires with applicable application and content offerings, allowing special offerings made on the basis of fine-grained customer demographics.

Entitlement Management systems in Action

There are many examples of organizations today that are leveraging Entitlement Management systems to solve a wide range of problems, regardless of their state of SOA adoption. In particular, organizations are applying Entitlement Management to solve a range of problems, such as:

Entitlement Management systems can automatically update user information whenever a change occurs.

- *Real-time information access* – Entitlement Management can enable users to access new Services as soon as they pay for them, order them, or complete whatever activities policies in place require them to complete in order to obtain access to the Service. Furthermore, Entitlement Management systems can automatically update user attributes whenever a change occurs, ensuring that information is current and accurate.

Example: cable TV customers can upgrade the level of service they receive via the cable provider's Web site in real time.

- *Real-time customer service* – Because Entitlement Management systems sit in the flow of the enterprise's applications, they can evaluate access policies in real-time, enabling the customer service representative's desktop to automatically pop up data on the customer's history at the field level from multiple data repositories.

Example: a 911 emergency operator can immediately see information on a caller as various queries complete, based upon caller ID and information the caller provides.

- *Real-time customer qualification* – When a user signs up for a new Service, Entitlement Management systems can verify the qualification of a customer, and perform operations such as running an immediate credit check. Based on the resulting information, the Service Provider would be able to either grant or deny access to content based upon current information. For example, such customer qualification is a fundamental anti-money laundering requirement for banks.

Copyright © 2007, ZapThink, LLC

Example: real-time online credit card application approvals.

- *Content and usage tracking* – Entitlement Management systems can track user access and usage for individual pieces of content or access to particular Services.

Example: collecting demographic data on customers of a consumer-oriented social networking site as they surf the various parts of the site.

- *Improved customer service across lines of business* – Most organizations, especially retail banking, struggle to provide a seamless customer experience across all the lines of business customers interact with, while simultaneously gaining insight into their most valuable customers. These companies struggle because they have isolated stovepipes of overlapping and isolated customer data, identity, and access control systems.

Example: Entitlement Management systems can enable on-line access to cross-organizational systems such as account balances, bill payment, credit and loan applications, and small business payroll services through a single Web-enabled interface via a single login and extended to all customer touch points such as ATMs and in-branch authentication devices.

- *Regulatory compliance* – In order to comply with regulations like the Gramm-Leach-Bliley and HIPAA acts, organizations must establish internal privacy standards that state that customers must be aware of what the organization is doing with their personal information and provide written approval for the use and sharing of such data within the organization.

Example: regulations such as the Sarbanes-Oxley act govern the use and sharing of financial information. Organizations must be able to determine if policies are adequate and audit activity to ensure compliance. Entitlement Management systems are a critical part of addressing such regulatory compliance issues by providing the control and visibility necessary to maintain regulatory compliance.

Entitlement Management: Integral Part of SOA Governance

The concept of *governance* is drawing substantial attention in corporate boardrooms and technical meetings alike, as companies struggle with complex regulatory compliance pressures, increasing globalization, enhanced competition, and the maturation of their markets. As a natural

Thank you for reading ZapThink research! ZapThink is an IT advisory and analysis firm that provides trusted advice and critical insight into the architectural and organizational changes brought about by the movement to XML, Web Services, and Service Orientation. We provide our three target audiences of IT vendors, service providers and end-users a clear roadmap for standards-based, loosely coupled distributed computing – a vision of IT meeting the needs of the agile business.

Earn rewards for reading ZapThink research! Visit www.zapthink.com/credit and enter the code **SECEMS.** We'll reward you with ZapCredits that you can use to obtain free research, ZapGear, and more! For more information about ZapThink products and services, please call us at +1-781-207-0203, or drop us an email at info@zapthink.com.

consequence, the concept of SOA governance is in the center of the spotlight today.

Enterprise architecture is a critical enabler of governance, and as companies adopt SOA as enterprise architecture, SOA governance becomes the primary way that companies can establish principles for the control of their organizations.

As the IT resources business users require become more flexible and generally better able to meet an increasingly broad range of business needs, IT becomes inextricably intertwined in the daily operations of the business. As such, enterprise architecture becomes a critical enabler of governance, and as companies adopt SOA as enterprise architecture, SOA governance becomes the primary way that companies can establish principles for the control of their organizations.

SOA governance focuses on the creation, communication, and enforcement of Service policies. Service policies are metadata that consist of a set of constraints and capabilities that govern how Services and their consumers interact, including the access policies that Entitlement Management deals with. SOA governance requires that organizations take business policies, typically in written form, and transform them into metadata-based rules that can help automate the process of validating and enforcing compliance with those policies both at runtime as well as design time. In order to be effective, companies must then manage policies through the entire Service lifecycle. Entitlement Management allows for the operationalization, review and auditing of access policies, which is a key component of governance.

To further illustrate the close relationship between Entitlement Management and SOA, it's important to note that the examples of Entitlement Management in the section above illustrate that fine-grained entitlements leverage the ability of an organization to abstract data as well as functional capabilities as Services. Entitlement Management systems can secure discrete data as well as specific application functionality, but by creating loosely coupled, contracted interfaces for those capabilities, an organization gains far more flexibility than a tightly coupled approach would provide.

To achieve the promise of SOA, it is also imperative that critical non-functional capabilities like security should be represented as Services.

Furthermore, to achieve the promise of SOA, it is also imperative that critical non-functional capabilities, in particular security, should also be represented as Services. It's important for the architect to externalize security capabilities as Services in order to improve the manageability and accessibility of the security capabilities in the organization.

There are several motivations for externalizing security as a set of Services. First, the security context for invoking individual Services is critical for providing the context of the Service-Oriented Business Applications (SOBAs), which are the composite applications that incorporate those Services. Second, the owners and administrators for the access policies that apply to various Services are typically different from the people developing the business logic for each Service. In fact, these people are often in different parts of the organization. Therefore, requiring the creation of access policy management at the same time as the business logic is rarely practical or efficient.

Finally, it is frequently necessary to audit access policies separately from the Services for compliance purposes. Organizations often require access policy auditing for each Service, as well as for the SOBAs that compose those Services. Note the in a Service-oriented environment, it's possible to invoke Services in diverse and unpredictable ways. Auditing is necessary for anticipating problems before they occur as well as for identifying the root cause of problems when they do occur. In, fact, in a properly designed

Copyright © 2007, ZapThink, LLC

SOA implementation, access policy management is itself an important set of Services.

Policy externalization enables administrators to change access policies to comply with changing security or compliance requirements without requiring any change to the Service.

The benefits of separating the access policy administration, enforcement, and auditing from the Services themselves is that such externalization enables administrators to change access policies to comply with changing security or compliance requirements without requiring any change to the Service, thus preserving the loose coupling of the Service. Furthermore, changing a particular Service generally won't require a change to its associated policies.

The secret to creating Services with externalized policy management is to avoid embedding policy management capabilities into the components underlying the Services. Instead, organizations must create Services that support the ability for standards-based "interceptors" that are able to permit or deny access to a Service through control of the invocation of the container interface that corresponds to the Service component. Such interceptors can be part of a Web Services-based SOAP stack, or more generally, Services can invoke external policy resolution Services regardless of the protocol or interface type to retrieve the access policy decision.

Since many different parties can control access policies, it is also important that the policy administration Service have a delegation capability. To maintain agility, different people may need to define different parts of individual policies at different times. Furthermore, there must be policies in place that govern which roles can administer which policies, so that when the person logs into the administration Service they should only be able to administer those aspects of each access policy that they are permitted to administer. The administration infrastructure Service should also be able to handle access policy conflicts.

III. Securent: Entitlement Management Designed for SOA

Addressing the need for Entitlement Management in SOA is Securent. Securent has developed the *Securent Entitlement Management Solution* (EMS), which simplifies the process of developing, administering, enforcing and auditing fine-grained entitlements by externalizing security policies from application logic. Securent also delivers such Entitlement Management capabilities as standards-based Services as well, providing Entitlement Management both for Services as well as through Services. Securent is thus able to address enterprises' need for fine-grained authorization, straightforward auditing to ensure compliance, and the overarching business need to reduce the IT costs associated with custom coding.

Securent is able to address enterprises' need for fine-grained authorization, straightforward auditing to ensure compliance, and the overarching business need to reduce the IT costs associated with custom coding.

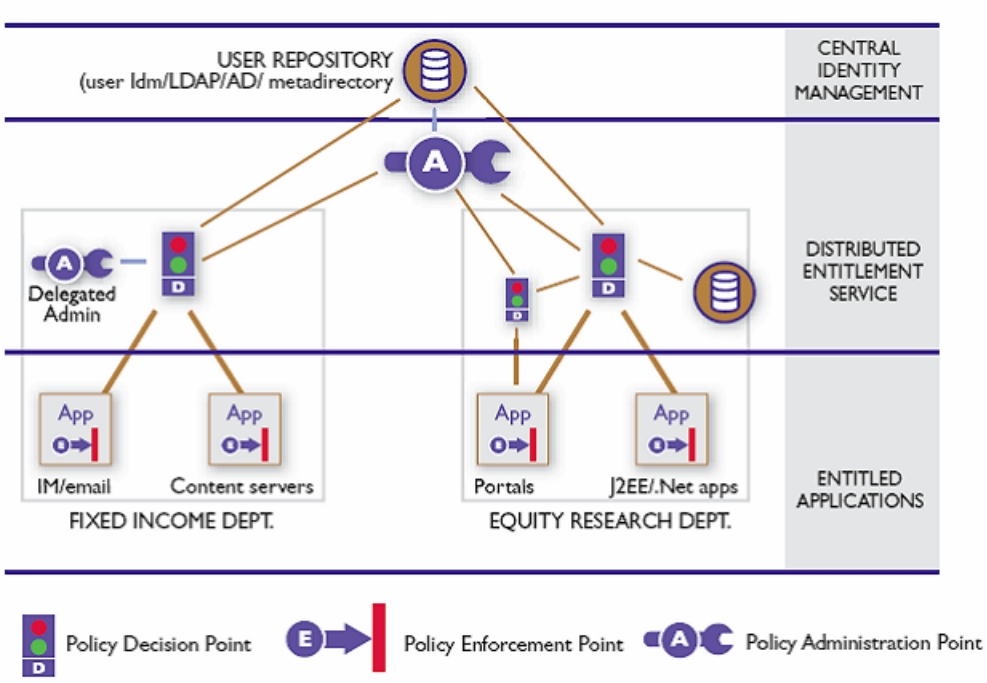
The core of Securent's solution is its ability to provide fine-grained security. Securent EMS offers fine-grained authorization, rich policy expressions, and entitlement auditing, reducing the costs, delays, brittleness, complexity, and risks associated with custom coding of entitlement policies. Securent EMS offers several IT administration capabilities, including delegated authorization management as well as centralized administration of the distributed authorization engines, offered as Services.

Securent EMS enables multiple owners of access policies, including application, security, and compliance teams to independently administer and configure the access policies, and also supports centralized audit and

Copyright © 2007, ZapThink, LLC

compliance teams to get access to aggregated data to generate appropriate reports. An illustration of the Securent EMS architecture protecting specific banking applications is shown in the figure below:

Securent Entitlement Management System



Source: Securent

In addition to deploying Securent EMS to provide consistent per-application and enterprise-wide policies in support of centralized Service consumers like corporate portals, Securent EMS can also help to secure commercial off-the-shelf applications such as enterprise collaboration and messaging systems. Since enterprises rely on collaborative electronic communications among employees, customers, and partners in an environment of heightened security and compliance, it's becoming increasingly important to leverage entitlement security solutions that can manage, enforce, and audit access consistently across various communication channels, including instant messaging, voice over IP, email, video conferencing, and the like.

Enforcing policies and controlling access while at the same time empowering users to meet the changing needs of the business is a central challenge for IT.

In this collaborative environment, enforcing policies and controlling access while at the same time empowering users to meet the changing needs of the business is a central challenge for IT. Enterprises must control access based on a number of attributes, including user profile attributes, environmental attributes, and others, without having to fall back onto custom coding security policy into each individual application. To solve this problem, Securent EMS externalizes fine-grained authorization policy from core application logic and delivers it as a Service, without the need to modify existing applications, by leveraging open standards like the Extensible Access Control Markup Language (XACML). As a result, Securent EMS provides the necessary Entitlement Management

Copyright © 2007, ZapThink, LLC

capabilities for organizations as they roll out Services as part of an enterprise SOA initiative.

IV. The ZapThink Take

Through 2006, the term *policy* has largely eclipsed the term *entitlement*, as SOA governance has focused almost entirely on policy creation, communication, and enforcement. Yet at its most basic, an entitlement is a policy, and thus Entitlement Management is a subset of the policy management aspect of governance. This fact begs the question as to whether speaking of entitlements separately from a general discussion of SOA governance adds value to the discourse.

It is vitally important for enterprises to focus on Entitlement Management as a separate endeavor from general SOA governance, as well as an integral part of such governance.

ZapThink believes, in fact, that it is vitally important for enterprises to focus on Entitlement Management as a separate endeavor from general SOA governance, as well as an integral part of such governance. The reason for this dual focus concerns the different levels of granularity that underlie the two subject areas. In the case of SOA governance, architects should be focusing primarily on policies as they apply to coarse-grained business Services. As a result, those policies themselves tend to be coarse-grained, as they apply to one or more such Services. In the world of entitlements, however, the focus is on *fine-grained* access control. One coarse-grained business Service might provide access to a broad range of data and functionality, depending upon its purpose, and yet those data and function points may require many separate entitlements that the organization must manage differently from how they manage the coarser-grained policies.

Technically, then, Entitlement Management is a subset of SOA governance, but in practice, these problem areas present different challenges that require different tools. This reason alone is sufficient for organizations who are implementing SOA to look at Securent EMS, if only to cover all of the issues that SOA governance presents. As such organizations come to understand the role Entitlement Management has in an overall SOA governance strategy, they will also be able to leverage the specific capabilities of Securent EMS for providing flexible, scalable management of fine-grained access control across all applications in the organization, regardless of whether they are Service-oriented or not.

Copyright © 2007, ZapThink, LLC

Copyright, Trademark Notice, and Statement of Opinion

All Contents Copyright © 2007 ZapThink, LLC. All rights reserved. The information contained herein has been obtained from sources believed to be reliable. ZapThink disclaims all warranties as to the accuracy, completeness or adequacy of such information. ZapThink shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice. All trademarks, service marks, and trade names are trademarked by their respective owners and ZapThink makes no claims to these names.

About ZapThink, LLC

ZapThink is an IT advisory and analysis firm that provides trusted advice and critical insight into the architectural and organizational changes brought about by the movement to XML, Web Services, and Service Orientation. We provide our three target audiences of IT vendors, service providers and end-users a clear roadmap for standards-based, loosely coupled distributed computing – a vision of IT meeting the needs of the agile business.

ZapThink helps its customers in three ways: by helping companies understand IT products and services in the context of Service-Oriented Architecture (SOA) and the vision of Service Orientation, by providing guidance into emerging best practices for Web Services and SOA adoption, and by bringing together all our audiences into a network that provides business value and expertise to each member of the network.

ZapThink provides market intelligence to IT vendors and professional services firms that offer XML and Web Services-based products and services in order to help them understand their competitive landscape, plan their product roadmaps, and communicate their value proposition to their customers within the context of Service Orientation.

ZapThink provides guidance and expertise to professional services firms to help them grow and innovate their services as well as promote their capabilities to end-users and vendors looking to grow their businesses.

ZapThink also provides implementation intelligence to IT users who are seeking guidance and clarity into the best practices for planning and implementing SOA, including how to assemble the available products and services into a coherent plan.

ZapThink's senior analysts are widely regarded as the "go to analysts" for XML, Web Services, and SOA by vendors, end-users, and the press. Respected for their candid, insightful opinions, they are in great demand as speakers, and have presented at conferences and industry events around the world. They are among the most quoted industry analysts in the IT industry. ZapThink was founded in November 2000 and is headquartered in Baltimore, Maryland.

ZAPTHINK CONTACT:
ZapThink, LLC
108 Woodlawn Road
Baltimore, MD 21210
Phone: +1 (781) 207 0203
Fax: +1 (815) 301 3171
info@zapthink.com

ZapThink, LLC • 108 Woodlawn Road • Baltimore, MD 21210 • info@zapthink.com • www.zapthink.com