



eaglehawk

SBX Enigma™

Product Overview

Document Issue Date
Q2 2009

Issued By:
Eaglehawk Limited
PO Box 292
Georgetown, MA 01833
USA

sbxenigma@eaglehawk.com

Table of Contents

Product Synopsis	3
Enterprise Data Security Functionality	3
Authentication	3
Authorization	3
Gatekeeper to Data	4
Comprehensive Centralized Audit	5
Ways to Use SBX Enigma™	5
Responding to Queries re: User Permissions	5
Structural Disassembly & Dispersal of Key Data Components	5
Removing High-Value Elements from Data Structures	5
Enhancing & Refining Management of Enterprise User Populations	6
Supporting Centralized Enterprise Management of Apps & Services	6
Supporting Centralized Enterprise-wide Audit Activities	6
Using SBX Enigma™ - A Detailed Shared Service/SOA Example	6
Traditional Enterprise Data Environment	6
Introducing An Enterprise Shared/SOA Service	6
SBX Enigma™ Enterprise-Level Security	7

Product Synopsis

SBX Enigma™ (SBX) is a customer-hosted Web Service that provides a secure repository for any Enterprise seeking to manage access to and protect its data.

Accessible to Client Applications through the SBX Application Program Interface (API), SBX is an in-memory, object-oriented data management system. SBX provides advanced security functionality that enables complex Enterprise data environments to centralize and streamline authentication, access management, and audit processes.

Enterprise Data Security Functionality

Within a typical Enterprise data environment there generally are a multitude of dynamic components: numerous Client Applications serving a range of internal and external Organizations, each of which services large User/User Group populations, with everything operating from multiple geographic locations.

As an Enterprise attempts to leverage the value of its data assets by sharing these multi-faceted resources across the entire scope of its operations, e.g., through adoption of dynamic approaches such as a Service Oriented Architecture (SOA), difficult data security issues arise that require comprehensive, flexible Enterprise-wide solutions. IT security, which traditionally focuses on each discrete legacy resource and its defined set of users, must evolve to support Enterprise-level services which, by definition, package previously autonomous components and cut across established resource and user boundaries.

Responding to both traditional and emerging Enterprise data security challenges, SBX provides functionality in the following areas:

Authentication

- SBX augments existing ID Management systems with **an additional, Enterprise-wide layer of security** which is invoked when users seek access to protected data resources through supported Client Applications & SOA Services.
- Authentication is based on presentation of valid user credentials. Valid credentials (User ID and Password/Passphrase) are established by all users through secure SBX procedures.

Authorization

- Successful authentication of an SBX **Administrative User** results in **Role-Based authorization** to access a strictly defined (and limited) sub-set of system functions, e.g., Enterprise Metadata Administrators gain access to Enterprise Metadata Maintenance functions, Organization User Managers gain access to Organization User Maintenance functions, etc.

The SBX Role-Based Administrative Framework is a failsafe-like construct that is specifically designed to minimize security risks associated with internal abuse by separating and distributing access to key functions. In this regard, **access privileges are constrained by an administrative user's Role** which, in turn, is functionally separated from other administrative Roles by the following categories:

- System Administration
 - Organization Administration
 - Metadata Administration
 - User Administration
 - Data Administration
 - Audit Administration
- Successful authentication of a **non-administrative Limited User** results in **User Group-Based authorization** to access specifically permitted Metadata Objects and Data Element Objects secured by SBX. User Groups are composed of non-administrative Limited Users.

Each discrete Metadata or Data Object has an Access Control List (ACL) specifying the User Group(s) with access privileges. Membership in such an authorized User Group is required for a Limited User to be granted access to the Object.

Gatekeeper to Data

In response to query calls it receives, SBX provides Client Applications & SOA Services with **Fine-Grained Access Control** over data resources across the Enterprise.

- **Metadata Object Access Control:** Within the context of an Enterprise data architecture **SBX Metadata can be viewed as a blueprint** that describes the underlying Enterprise data assets and their organization. The Metadata blueprint includes all Enterprise data assets, their types, locations, storage methods, and thereby provides a way to describe the aggregate Enterprise data architecture.

By incorporating ACLs for all components of the Enterprise data architecture into the Metadata blueprint, SBX supports access management and control across that architecture down to the level of individual components. SBX responds to Application/Service queries regarding user access permissions to Metadata Objects as follows:

- Querying through the SBX API, the Application/Service requests SBX to provide the user's access authority to the sought-after Metadata Objects.
 - Responding through the API, SBX confirms or denies the user's authority to access, first, the data structure (e.g., the database) and, second, specific components (e.g., database tables and fields) within that structure.
- **Data Element Object Access Control:** SBX provides Client Applications & SOA Services with the ability to remove **high-value data elements** (e.g., Personally Identifiable Information, encryption keys) from their typical location in database tables and safeguard them as discrete Data Element Objects in SBX. Subsequent access to these high-value data elements is authorized or denied based on the discrete Access Control List of each such Data Element Object.

SBX responds to Application/Service queries regarding user access permissions to Data Element Objects secured within SBX by confirming or denying user authority to access these specified Data Element Objects – i.e., **need-to-know authority**.

Using this approach, SBX can be utilized to manage and authorize almost any named Enterprise asset.

- Confirm/deny user authority to access a specified Client Application or SOA Service
- Confirm/deny user authority to access other Enterprise resources – e.g., servers, data centers
- Confirm/deny user authority to access storage elements and components – e.g., folders, files

Comprehensive Centralized Audit

SBX simplifies audit procedures through standardization of Enterprise-wide audit processes available to all Enterprise Client Applications & SOA Services, thus providing for real-time identification and monitoring of Enterprise-wide resource usage through:

- Comprehensive, mandatory audit of administrative activities
- Flexible, optional audit of SBX interactions with Client Applications and SOA Services
- Generic, as-required audit of any independent Client Application/Service event.

Ways to Use SBX Enigma™

Because of the significant flexibility SBX Enigma™ provides –control over how users are organized & managed, how data is described, what types of data are managed, and how/what is audited - there is a broad range of ways in which SBX Enigma™ functionality may be employed. Several of the most common uses include:

Responding to Enterprise application/service queries re: user access permissions

- Confirm/deny user access authority to specified applications/services – e.g., SOA components
- Confirm/deny user access authority to data structures and components within those structures – e.g., folders, files, databases, tables, fields
- Confirm/deny user access authority to other Enterprise resources – e.g., servers, data centers
- Confirm/deny user access authority to specified data elements – e.g., need-to-know authority

Securing data through structural disassembly & dispersal of key components

- Disassemble data structures into components – e.g., redacted documents, images, database tables – and store these components in multiple locations
- Secure the location pointers in SBX Enigma™

Securing high-value data elements by removing them from data structures

- Identify & remove high-value data elements and components – e.g., SSNs, DOBs, encryption keys – from their data structures
- Secure the removed data elements and components in SBX Enigma™

Enhancing & refining the management of Enterprise User Populations

- Augment existing ID Management systems with an additional layer of security
- Expand the flexibility & security of access management across both established and new User/Role classifications
- Institute/improve security safeguards against “permission creep”
- Decrease the potential for internal security abuse through limitations on, and overlapping responsibility for, key administrative functions

Supporting centralized management over Enterprise data applications/services

- Facilitate the creation of Enterprise-wide standards and naming conventions
- Enable the centralized administration of access to Enterprise data

Supporting centralized Enterprise-wide audit activities

- Identify inappropriate access across Enterprise data structures
- Identify and monitor Enterprise resource usage
- Provide for real-time monitoring

Using SBX Enigma™ - A Detailed Shared Service/SOA Example

Traditional Enterprise Data Environment

Looking first at a simplified example of Enterprise architecture, Figure 1 shows a basic Enterprise configuration where autonomous systems are established for Finance, Logistics, and CRM.

In turn, access to each of these systems is autonomously managed at the system, or Community of Interest (COI), level, resulting in discrete sets of resource-specific Users and User Groups for Finance, Logistics and CRM.

When a User seeks access to a particular

resource, they undergo an Authentication process wherein identifying credentials (e.g., a User ID and Password) are presented.

Validation of the credentials result in establishment of the User’s authorization level and, based on this authorization, access is controlled at the resource level.

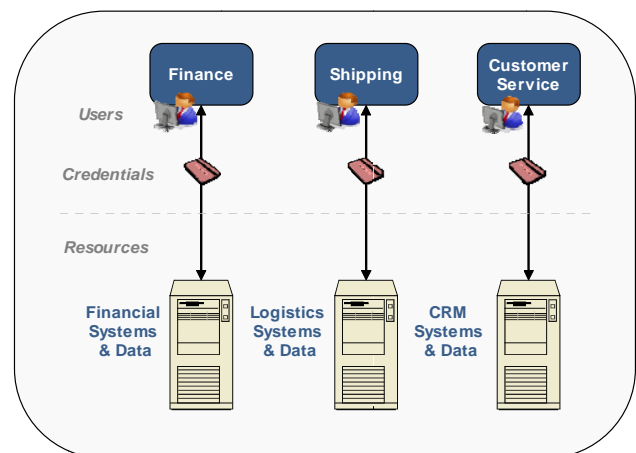


Figure 1 – Traditional Enterprise Data Environment

Introducing An Enterprise Shared/SOA Service

In order to leverage the potential value of the autonomous resources portrayed in Figure 1, the Enterprise in this example decides to adopt a shared SOA-type approach for a new service wherein components from the various legacy systems can be packaged together to meet a service requirement that spreads across traditional resource boundaries.

In this example, the Enterprise wishes to establish a new shared service that supports a Product Upgrade Program. This Program will be implemented by customer-facing Sales and Customer Service staff, and will require access to data from all three of the underlying resources to determine the eligibility of specific customers for the Program.

Specifically, CRM data will be accessed to ascertain existing product configurations, Financial data will be accessed to identify customer credit details, and Logistics data will be accessed to determine product availability in the customer's geographic location. The required architecture for the Product Upgrade Service is depicted in Figure 2.

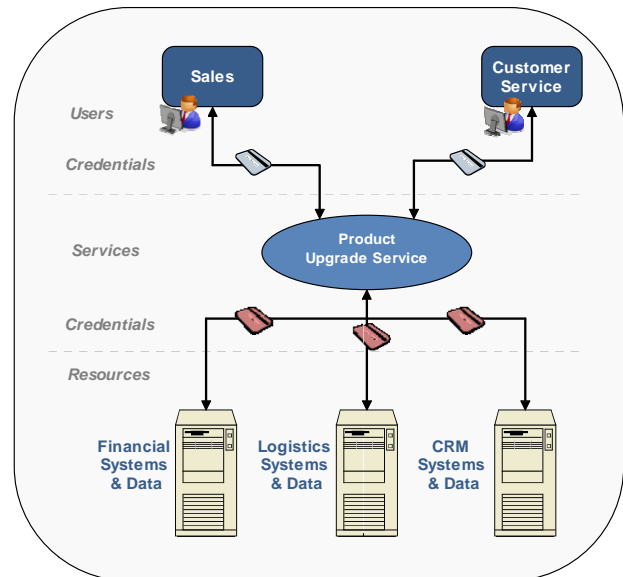


Figure 2 – Shared/SOA Service to Support Product Upgrades

As shown, introduction of the new Shared/SOA Service is accompanied by a new set of Authentication, Authorization, and Access Control requirements vis-à-vis the underlying resources. Stated differently, since it is entirely plausible that the Users of the new service, i.e., Sales & Customer Service reps, currently have limited or no access to the underlying Finance, Logistics, and CRM resources, a new methodology must be introduced that both supports the requirements of the new service while maintaining security over the underlying resources.

It is important to emphasize two fundamental points that are reflected in this example. First, introduction of the new service does not disrupt or impact the underlying legacy resources. The new service is simply elevated above these resources to enable these resources to be leveraged through sharing across the entire Enterprise.

Second, the established data security protections employed by these legacy resources likewise need not be disrupted. What is required, however, is an elevation in the scope of data security to address the Enterprise-level requirements created by resource sharing across traditional boundaries. Optimally this elevation will retain the existing COI-level management of access – i.e., control of the legacy resources will continue to be aligned with data ownership – while facilitating an expansion of access to support the objectives of the new service.

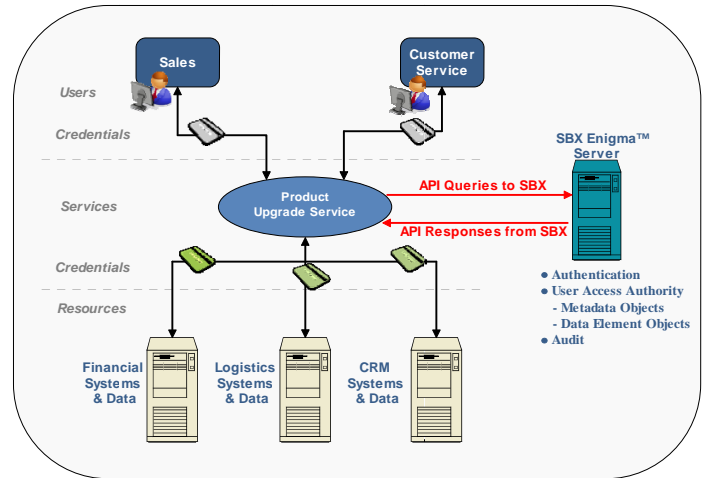
SBX Enigma™ Enterprise-Level Security

The central data security challenges that arise with the Product Upgrade Service depicted in Figure 2 are related to the management of access by users of that service to the underlying legacy resources.

In this example, users that previously had limited or no authority to access Finance, Logistics, or CRM resources must now be granted access permissions to specific components within those resources. In short, the challenges include Authentication of an

Enterprise-wide set of users and establishing the Authorization, or Access Privileges, of those users to access specific components from the underlying legacy resources.

As shown in Figure 3, SBX provides a solution to the specific data security challenges created in this example. Through query/response interactions between the Product Upgrade Service and SBX, user Authentication and User Access Authorities are established in a manner that supports centralized Enterprise-wide access management. Additionally, standardized SBX Audit processes are pervasive throughout such interactions and support centralized audit management and control.

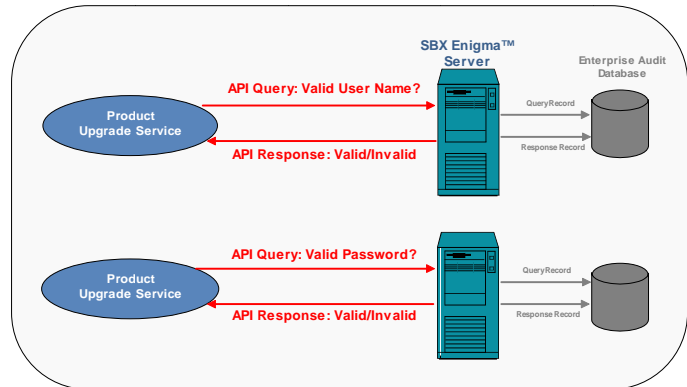


**Figure 3 – SBX Enigma™
Fine-Grained Access Control**

Looking more closely at SBX utilization, the initial step in the process involves Authentication. All users seeking access to resources protected by SBX must first undergo this process, which is depicted in Figure 4.

As shown in this example, a user attempts to log into the Product Upgrade service by providing, first, a User ID and, second, a Password. At each step in this process, the Product Upgrade Service queries SBX to determine validity.

At each interaction between the Product Upgrade Service and SBX, an audit record of the event is created and stored in the Enterprise Audit Database.



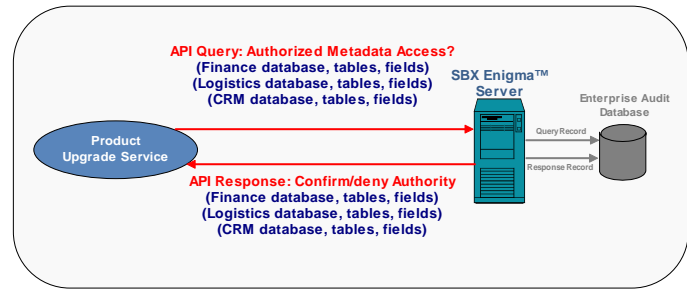
**Figure 4 – SBX Enigma™
Authentication**

Following successful Authentication, the user's Access Privileges are established based on the User Groups to which they belong. In this example, it can be assumed that there are two User Groups associated with the Product Upgrade Service: Representatives, comprised of Sales and Customer Service reps, and Managers, comprised of Sales and Customer Service Managers.

After successful Authentication of the user, the Product Upgrade Service processes the user's request for access to specific data. This involves sending a query to SBX to determine the user's Fine-Grained Access Privileges, as depicted in Figures 5 & 6.

As shown in Figure 5, SBX employs a Metadata layer that can be viewed as a blueprint describing the underlying Enterprise data resources and their structure.

Based on the authenticated user's request, the Product Upgrade Service sends a query to SBX to determine the user's Metadata Access Authority. In this example, it can be assumed that users belonging to the Representatives User Group (i.e., Sales and Customer Service reps) have authority to access certain current product configuration details in the CRM database and geographic product availability details in the Logistics database.



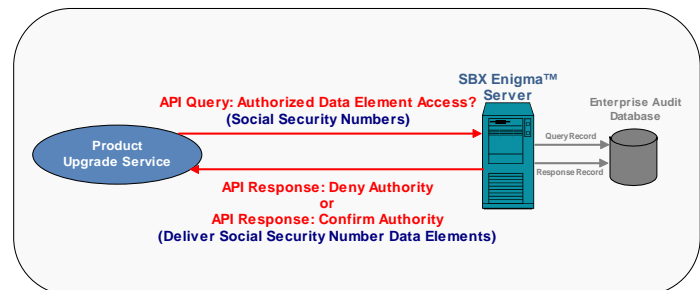
**Figure 5 – SBX Enigma™
Fine-Grained Access Control
Metadata Objects**

It is important to emphasize that no other components in either the CRM or Logistics databases are exposed to the Representatives User Group, and that this User Group has no access authority at all to the Finance database. It can be seen, therefore, that while legacy resources are being used to support the new service, exposure of those legacy resources is subject to Fine-Grained, Component-Level, access control.

Turning next to the Managers User Group, it has been assumed that this User Group has the same access privileges to the CRM and Logistics data structures as the Representatives User Group. In addition, however, the Managers User Group has access authority to Metadata components in the Finance database. Specifically, in order to approve a Product Upgrade for a specific customer, the Managers User Group has authority to access Metadata fields related to a customer's credit history, including the Social Security Number field.

For purposes of this example it is assumed that, unrelated to the process of establishing the new Shared/SOA Service, the Finance database has been separately secured by SBX and that Data Element Objects in the Social Security Number field (i.e., the actual Social Security Numbers for customers) have been removed from the Finance database and are stored in SBX.

Through the Fine-Grained Access Control process depicted in Figure 5, therefore, authenticated users belonging to the Managers User Group are authorized to access the Metadata field in the Finance database for Social Security Numbers. Following this authorization, when Data Elements from this field are requested a query is made to SBX and the requested Data Elements that are individually authorized are delivered as shown in Figure 6.



**Figure 6 – SBX Enigma™
Fine-Grained Access Control
Data Element Objects**

As shown in Figures 4, 5, and 6, all interactions between the new Product Upgrade Service and SBX result in the creation of Audit records that are entered into an Enterprise Audit database. SBX Audit processes are available to all Enterprise Applications and Services, and provide a simple, centralized and standardized means of identifying and monitoring Enterprise-wide resource usage in real-time.