



SBX Enigma™

Functional Components

1. Identification and Authentication

SBX Enigma™ requires that all user entities requiring access be uniquely identified and authorized. Users, applications and services are all examples of user entities (users) that need to be identified and authorized. User Groups may be created that provide for associating users with like access privileges. In order to reduce maintenance, import capabilities can be provided from an Enterprise's Active Directory facility.

2. Metadata

SBX Enigma™ metadata can describe the information and system assets of the enterprise. Data, file types, services, applications, servers, etc. can be described and arranged hierarchically so that access can be managed. Using metadata, users can be granted or denied access to the enterprise's information and system assets.

Data assets (databases) can be described regardless of their location in separate databases, thus providing a total view of an enterprise's database assets in one place. This capability simplifies administration of access to enterprise-wide data by reducing the requirement for individual database administration.

Applications and services can utilize this metadata information to provide knowledge of a user's access to construct and manage access to the enterprise assets. Applications and services can therefore be developed that are dynamic in nature, responding and delivering capabilities uniquely for each User.

By constructing a metadata representation of the services and/or system assets of an enterprise, applications and services can access the knowledge they need to direct or deny access to those assets.

3. Data Elements

Need-To-Know is a difficult capability to deliver in enterprise information systems. SBX Enigma™ provides data element management features with fine-grained access control delivering Need-To-Know capabilities.

Within SBX, the data element repository can be viewed as a collection of LockBoxes containing data elements. Each LockBox is described in SBX Enigma™ metadata, with a unique identity and can hold up to four uniquely identified individual data elements. It is assumed that data elements held by SBX Enigma™ are small (usually not exceeding about 50 characters), of high-value, and should be accessed only on a need-to-know basis, for example, Personally Identifiable Information, encryption keys, file names, server locations, URL's, etc. Access to

each SBXPK and Data Element held by SBX Enigma™ is managed by its own discrete Access Control List.

When SBX Enigma™ allocates a LockBox to a particular purpose, the its unique identity, or SBXPK (SBX Primary Key), is returned to the application for storage in some alternate location such as a database or, in highly sensitive circumstances, a separate SBX Enigma™ server.

Each SBXPK also has an Alias, available to an authorized user who knows the SBXPK value. This SBXPK Alias can be used as the primary key to child information in a Parent-Child relationship.

By disconnecting child data (e.g., transactions) from parent data (e.g., account holders), it is possible to secure large amounts of information that require specific access authorities to the parent's data (SBXPK) in order to access the child information (SBXPK Alias). In SBX Enigma™ there is no method for discovering a parent SBXPK value by knowing the child SBXPK Alias.

SBX Enigma™ data element capabilities allow individual organizations to design their own diverse and unique security mechanisms for their most valuable information assets. Ownership of an SBX Enigma™ environment provides no knowledge of how any other organization may be using it.

As an example, a User may have broad access to client Tax ID's (a metadata determination) but in order to access an individual Tax ID that has been stored in an SBX Enigma™ data element object, authorization must be granted on the individual Tax ID sought. In simple terms, this may mean that the user can generally access Tax ID's, except for certain Tax ID's of certain protected clients etc. These Need-To-Know protections, of course, are not limited to data sourced from a database but extend to *any* data held by SBX.

4. Audit

In addition to mandatory audit of all SBX Enigma™ administrative functions, the audit facilities of SBX Enigma™ provide for a comprehensive centralized audit facility for the whole enterprise. Most enterprises have many applications and services with audit capabilities. Review of user activity across the many auditable events in the enterprise for any individual user or group of users is often difficult and lacks the timeliness required for comprehensive oversight.

SBX Enigma's audit provides the framework and controls to provide fine-grained and targeted audit of all enterprise activity regardless of the diversity of auditable events.