



# SBX Enigma™

## Feature & Performance Assets

### SBX Enigma™ Datastore

1. SBX employs a single in-memory data persistence and application space which is dynamically protected/backed-up by snapshots of persistent objects written to disk at user-specified intervals.
2. SBX is impervious to attacker penetration.
  - a. Uninterrupted symmetry is required at all times.
  - b. Penetration/modification resulting in corruption of the persistent graph effectively denies access to SBX content in memory.
  - c. All content within persistent data element objects is encrypted.
3. Each data element is an individual object with its own discrete Access Control List (ACL).

### Data Structure & Organization

1. SBX employs a multi-component structure to optimize and secure access to data:
  - a. All SBX access flows first through a Metadata layer describing the data and its organization.
    - Each Metadata component of this description/organization is a discrete object.
    - Each object is protected by its own Access Control List (ACL).
  - b. Following authorized access through the Metadata layer, SBX evaluates access to individual data elements at the object level.
    - Each data element is an individual object with its own discrete ACL.
    - Access to the content of each discrete object requires a correctly formatted request from an authorized User on its ACL.
2. Access Control Lists & User Groups are dynamic and can be modified in real-time under program control.
  - a. Enables complex business rules to be applied for the granting of access authority, e.g., rules related to time-of-day, geographic location, shelf-life, etc.

### Audit

1. All creation and maintenance of Metadata is subject to audit (who, what, when).
2. All Web Service activity is subject to configurable, fine-grained audit. For example:
  - a. System access;
  - b. Creation, maintenance, and/or access to data elements.

### Web Service Access to SBX Enigma™

1. Within a Service Oriented Architecture (SOA), SBX is a Web Service accessible via XML-RPC using HTTP or HTTPS.
2. SBX is accessible to all Windows applications through the SBX API, which serves as the client application interface for authentication, message format & management.
3. SBX access & functionality is protected by dynamic session control, beginning with a 2-phase User authentication and continuing with every subsequent User interaction, i.e., SBX creates/requires new session ID for every User interaction.
4. SBX can be called by any Windows application to store high-value information and restrict any subsequent access to authorized Users, e.g.
  - a. high-risk data elements (SSN, date-of-birth, account identifiers),
  - b. encryption keys,
  - c. data table linkages, binary locators.

### Access Management & Administration

1. SBX separates access management rights and responsibilities into overlapping areas of authority designed to reduce the potential for the internal compromise of access security. To this end, five primary classes of users are utilized:
  - a. SBX System Administrator
    - Creates Organizations, creates the User Administrator, has no access to data elements.
  - b. User Administrator
    - Creates/removes the initial User Manager for each Organization.
  - c. User Manager
    - Creates/removes Data Managers, Users, User Groups, and additional User Managers, has no access to data elements. Manages import of Users and User Groups from Active Directories (LDAP).
  - d. Data Manager
    - When added to a User Group by User Manager, can access all data elements including those marked as deleted, therefore allowing for Restore functionality.
  - e. User
    - When added to User Group by User Manager, can access Metadata/data elements, cannot access data elements marked as deleted.