



Product Overview:

# SBX SecureShare™

## Managing High-Security File Sharing

SBX SecureShare™ is a browser-based application that provides comprehensive management control over the process of securely sharing sensitive files.

Designed for use in environments where security and privacy is important, SBX SecureShare™ separates the file sharing process into discrete functions at both the originating and receiving ends. This separation enables significant role-separation to be employed, enhancing process security, accountability, and efficiency.

A browser-based application, SBX SecureShare™ employs an easy-to-use graphical interface wherein the features and functions made available to users are determined by – and limited to – the user's role.

In addition to providing fine-grained control over all aspects of the file sharing process, SBX SecureShare™ provides a layered security framework with comprehensive accountability based on detailed audit tracking and reporting of all activities.

### Using SBX SecureShare™

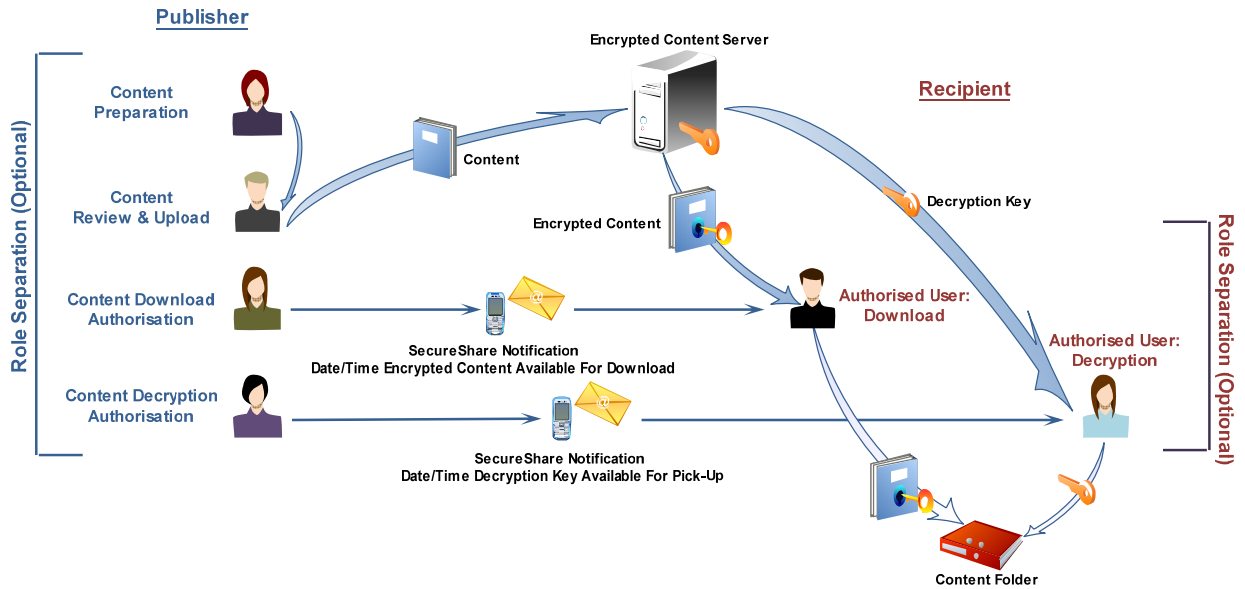
SBX SecureShare™ is designed for use in demanding security environments where granular process controls and role-separation contribute to strengthening of both internal and external security.

SBX SecureShare™ processes comprise three primary phases:

- Phase One - Identify files for sharing
- Phase Two - Authorise Recipients and notification of file availability
- Phase Three - Receipt of files



The following diagram provides a graphic overview of a typical file sharing event and highlights both the process and the (optional) role-separation that might be employed.



## **Phase One**

Create a description of the file, review and approve the content to be shared, and upload to an encrypted content server. Optional role-separation (file preparation/description, review and approval, upload) may be employed. The SBX SecureShare™ interface limits functionality to each user's role.

NOTE: The content to be shared has been prepared and secured through government-sanctioned encryption and remains under the Publisher's control.

## **Phase Two**

Recipient authorisation and notification, with an important distinction between two separate processes: download and decryption.

In the first instance, designated Recipients are authorized to download the encrypted file from the SecureShare™ content server. In the second instance, potentially different Recipients are authorized to decrypt the file that has been downloaded. In both cases, Recipients are notified through conventional email or SMS that SecureShare™ material is available for pick-up between X and Y (dates & times).

The distinction between the download and decryption processes enables the Publisher to control who-does-what at the Recipient end, e.g., the assistant is granted download authority but only the executive has decryption authority. Additionally, the Publisher can control when events occur,



e.g., a press release or proposal may be downloaded immediately but can only be decrypted next Tuesday between 8:00 and 8:15.

NOTE: At this stage, the encrypted content to be shared is still resident in the Publisher's environment.

### **Phase Three**

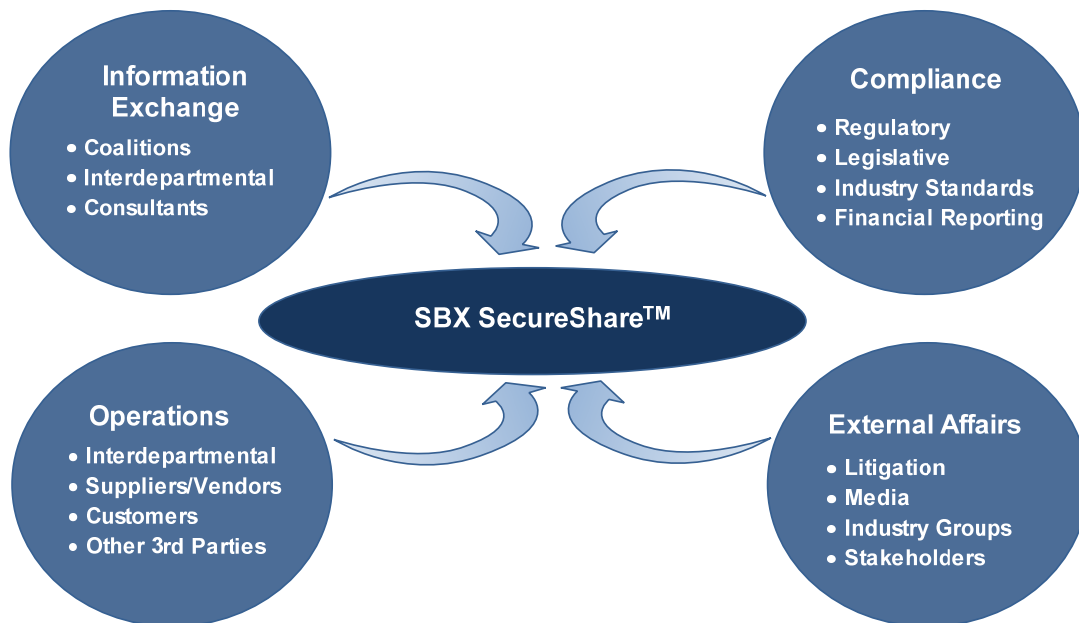
Download of the encrypted content and download of the decryption key. It is important to note that these are distinct events optionally involving separately authorised users and, potentially, separate timeframes.

When the Recipient, who must be logged in and authenticated by SecureShare™, selects the file/key for download, they are actually interacting with the SBX security framework which evaluates the Recipient's access privileges and authorizes a download of the encrypted file and/or the decryption key associated with the file. It is only after download of the decryption key to the Recipient that the encrypted content is decrypted.

NOTE: Upon download of the encrypted file and decryption key to the Recipient, the SecureShare™ event is completed. Any restrictions that the Publisher placed on the original file – separate authentication requirements or rules such as no-copy, no-print, no-paste, no-save, etc. – will be retained in the Recipient's copy of the file.

FINAL NOTE: The Publisher, for whatever reason, may revoke the download and/or decryption process at any point prior to the Recipient's actual download of the file and decryption key.

## **The Secure Management of High-Value File Sharing**





## Key Features of SBX SecureShare™

SBX SecureShare™ combines layered security and rigorous process controls with optional fine-grained role-separation.

### Operating Features

- |  |  |
|--|--|
| <ul style="list-style-type: none"><li>• <b>No Client Software Required</b></li></ul> | Entirely browser-based, eliminates installation & on-going maintenance of client software  |
| <hr/>  |  |
| <ul style="list-style-type: none"><li>• <b>Role Separation</b></li></ul>             | Publisher: <ul style="list-style-type: none"><li>▪ File Description Preparation</li><li>▪ Review, Approval</li><li>▪ File Encryption and Upload</li><li>▪ Download Authorisation(s)</li><li>▪ Decryption Authorisation(s)</li><li>▪ Download, Decryption Notification(s)</li></ul> Recipient: <ul style="list-style-type: none"><li>▪ Download of Encrypted File</li><li>▪ Decryption of Downloaded File</li></ul> |
| <hr/>  |  |
| <ul style="list-style-type: none"><li>• <b>Intuitive, Role-Based GUI</b></li></ul>   | Available functions dictated by the user's role  |
| <hr/>  |  |
| <ul style="list-style-type: none"><li>• <b>Recipient Process Controls</b></li></ul>  | Download: <ul style="list-style-type: none"><li>▪ When Encrypted File Is Available</li><li>▪ How Long Encrypted File Is Available</li></ul> Decryption: <ul style="list-style-type: none"><li>▪ When Decryption Key Is Available</li><li>▪ How Long Decryption Key Is Available</li></ul>  |
| <hr/>  |  |
| <ul style="list-style-type: none"><li>• <b>No Size Limits</b></li></ul>              | No size limits on shared files   |
| <hr/>  |  |
| <ul style="list-style-type: none"><li>• <b>Notifications</b></li></ul>               | Email and/or (optionally) SMS: <ul style="list-style-type: none"><li>▪ Download Availability</li><li>▪ Decryption Key Availability</li></ul>   |
| <hr/>  |  |
| <ul style="list-style-type: none"><li>• <b>Revocation</b></li></ul>                  | Revocation at any point prior to: <ul style="list-style-type: none"><li>▪ Download</li><li>▪ Decryption</li></ul>  |
| <hr/>  |  |
| <ul style="list-style-type: none"><li>• <b>Real-Time Status Reporting</b></li></ul>  | All activity on a file sharing event   |



### **Security Features**

• <b>Government-Level Encryption</b>	AES 256
• <b>Encryption Processes</b>	Message and file attachment encryption
• <b>Files/Decryption Keys Retrieved, Not Sent</b>	Message waiting notifications sent, but only registered users can retrieve actual files/decryption keys after logging in and being authenticated
• <b>Integrated Access Management</b>	Access control and data protection capabilities of SBX Enigma™ technology – CC EAL 2+
• <b>Preservation of File Properties</b>	All shared files preserve their original properties (authentication, no-print, no-copy, no-paste, no-save, etc.)
• <b>Comprehensive Audit</b>	Fine-grained audit of all Publisher and Recipient activities

## **The Role of SBX Enigma™ Technology**

Underlying all SecureShare™ processes is a pervasive security framework managed by SBX Enigma™, a Common Criteria certified technology providing exceptional access control and data protection functionality.

The security functions of SBX Enigma™ are employed at essentially every step in the SecureShare™ file sharing process, including:

- Authentication of all users,
- Management of content/file identities,
- Management of all encryption keys,
- Authorization of all sharing, notification, download & decryption activities.
- Audit of all events

The following diagram provides a snapshot of the primary interactions with SBX Enigma™ emphasizing the comprehensive nature of the security framework integrated throughout SBX SecureShare™.

