Centrix Single Sign-on Overview

Glossary of Terms

- ETMS = ExactTMS positive pay system
- SSO = Single Sign-On
- OLB/Requestor = Online Banking Application
- User Id = ETMS User Id
- System Id Code = System Identification Code

The Exact/TMS positive pay system supports single sign-on from other online banking applications . For example, if a business customer is already logged on to the bank’s online business banking application and the user next wants to go into ETMS, the user can simply click on a link within the online banking application to access the ETMS screens without having to perform a second login to ETMS. In order to accomplish this, the other online application must perform a series of steps to authenticate both the system performing the request and the user within ETMS.

Data Elements

The requesting application must permanently store three data elements required for the SSO processing – a 16 character system identification code, a 32 character encryption key, and a 16 character initialization vector value. AES encryption is used within the single sign-on processing. The following parameters are used for the AES encryption:

- Block / Initialization Vector (IV) Size: 128 bits (16 bytes)
- Encryption Key Size: 256 bits (32 bytes)
- Cipher Mode: CBC
- Padding: PKCS7

Basic Message Flow

1. The requestor sends a message to ETMS requesting a one time password key. On the request message, the requestor includes a System Id Code that enables ETMS to identify the requesting system and the ETMS User Id requesting an SSO.
   a. Both the System Id Code & and the ETMS User Id may optionally be encrypted. The same encryption methods used to encrypt the password would also be used to encrypt either of these incoming values.
2. The requestor receives a response from ETMS with the one time password key. The one time password key is not encrypted in the response. The one time password key expires after one minute.
3. The requestor uses the one time password key and the encryption key value(s) to create an SSO login password. The AES encryption key and AES initialization vector values are private values that are never transmitted on messages between the requestor and ETMS.
4. The requestor sends an SSO request message that includes the User ID and the encrypted login password. The password should be Base64 encoded and the Base64 encoded value should be URL encoded prior to sending the SSO request.
   a. As mentioned previously, the User Id may optionally be encrypted. If encrypted, the User Id password should be Base64 encoded and the Base64 encoded value should be URL encoded prior to sending the SSO request.
5. ETMS validates the user and the SSO login user ID and password. The one time password is cleared and may not be used for future SSO requests.

Single Sign-On Messages

The messaging for the SSO process is all handled via the HTTPS protocol. Fields values are transmitted by via HTTP GET messages. Specific field names are required within each request.

One Time Password Key Request Message

The sign sign-on login page is:

https://**<domain name of Exact/TMS>**/Pages/otpwd.aspx?u=**<User ID>**&s=**<System Id Code>**

The following fields are required on the one time password key request message:

User ID – contains the User Id of the person requesting the sign-on to ETMS. The User Id passed to ETMS, must match up to an existing ETMS active user in order for a one-time password to be returned.

System Id Code – contains the System Id Code. A unique 16 digit numeric system identification code will be assigned to each financial institution using the single sign-on interface.

> ***Note*****:** If either the User Id and/or System Id Code are encrypted, the encrypted values should be Base64 encoded and the Base64 encoded value should be URL encoded prior to sending the SSO request.

One Time Password Key Response Message(s)

The following text will be returned within an HTML document to the requestor for each **successful** one-time password request:

<otpwd>**999999999999999**</otpwd>

999999999999999 represents the unencrypted one-time password.

The following text will be returned within an HTML document to the requestor for each **rejected** one-time password request:

<errorcode>**9999**</errorcode><errormessage>**Error Message Text**</errormessage>

9999 represents the error code associated with the reason the request was rejected.

Error Message Text represents the reason the request was rejected.

Error Codes

The following errors may be returned by the one-time password request message:

Error Code	Error Message
0001	System does not support single sign-on
1001	Invalid User ID Code
1002	Invalid System ID Code
1003	Missing User ID Code
1004	Missing System ID Code
1005	Missing Password
1006	One Time Password has expired
1007	User is Locked

Single Sign-on Login Request Message

After the one time password key is received, the requestor must create an encrypted password value by sending the one time password, the AES encryption key, and the AES Initialization Vector value through an AES encryption routine.

The single sign-on login page is:

https://**<domain name of Exact/TMS>**/Pages/loginsso.aspx?u=**<User ID>**&p=**<Encrypted One Time Password Value>**&i=**<Session Keep Alive Image URL>**

The following fields are required on the single sign-on login request message:

User ID – contains the ExactTMS user ID of the person requesting the sign-on to the Exact/TMS system. A user record which with a matching user ID will need to be defined in the Exact/TMS system in order for a one-time password to be returned.

> ***Note*****:** If User Id is encrypted, the encrypted value should be Base64 encoded and the Base64 encoded value should be URL encoded prior to sending the SSO request.

Encrypted One Time Password – contains the encrypted one time password value. The encrypted value should be Base64 encoded and the Base64 encoded value should be URL encoded prior to sending the SSO request.

Session Keep Alive Image URL – the full URL (Ex: http://www.samplebank.com/onlinebanking/image/keepalive.gif) of an image file on the requesting system's website. Each time an ETMS menu option is clicked, the ETMS system will get this image. The purpose of this is to keep the requesting system's session active while the user is working in ETMS. The image file that this URL points to should be a 1 pixel X 1 pixel PNG image file. This parameter is optional.

Exact/TMS will be responsible for displaying the reply page to the single sign-on login request message. The system will either display the system home page to the user or display an error message in the browser window.

Encryption Example

The following data elements were used in this example:

AES Encryption Key: 1234567890ABCDEF1234567890ABCDEF

AES Initialization Vector (IV): 1234567890ABCDEF

System Id Code: 1234567890123456

User Id: tuser

Sample One Time Password Key Request Message

No values encrypted

https://www.Centrix.com/ExactTMS/Pages/otpwd.aspx?u=**tuser**&s=**1234567890123456**

User Id encrypted (optional)

https://www.Centrix.com/ExactTMS/Pages/otpwd.aspx?u=**Wc4I/cu3KbetLGtqANmwWg==**&s=**1234567890123456**

Unencrypted User Id	Encrypted User Id
tuser	Wc4I/cu3KbetLGtqANmwWg==

System Id Code encrypted (optional)

https://www.Centrix.com/ExactTMS/Pages/otpwd.aspx?u=**tuser**&s=**5Fr/gQmtq6wp8RY1COldAhELchTPqMQBajLALP1tfOM=**

Unencrypted System Id Code	Encrypted System Id Code
1234567890123456	5Fr/gQmtq6wp8RY1COldAhELchTPqMQBajLALP1tfOM=

Both User Id & System Id Code encrypted

https://www.Centrix.com/ExactTMS/Pages/otpwd.aspx?u=**Wc4I/cu3KbetLGtqANmwWg==**&s=**5Fr/gQmtq6wp8RY1COldAhELchTPqMQBajLALP1tfOM=**

Sample One Time Password Key Response Message

<otpwd>**2142377673635265**</otpwd>

Sample Single Sign-on Login Request Message

No values encrypted

https://www.Centrix.com/ExactTMS/Pages/LoginSSO.aspx?u=**tuser**&p=**rGT9KGTA4t9IJ7LEuUfh09dfiKdsKs3h0nYvU64jPy4=**

Unencrypted Password	Encrypted Password
2142377673635265	rGT9KGTA4t9IJ7LEuUfh09dfiKdsKs3h0nYvU64jPy4=

User Id encrypted

https://www.Centrix.com/ExactTMS/Pages/LoginSSO.aspx?u=**Wc4I/cu3KbetLGtqANmwWg==**&p=**rGT9KGTA4t9IJ7LEuUfh09dfiKdsKs3h0nYvU64jPy4=**

Important note about encrypting User Id

If the Financial Institution and OLB provider decide to use the option to pass an encrypted user Id, when the requestor passes the encrypted User Id, the User Id value they encrypt, will need to exactly match the case of the User Id setup within ETMS.

Example

Unencrypted	Encrypted
tuser	Wc4I/cu3KbetLGtqANmwWg==
TUSER	C18oG1wgT6RxBGW70A7/cg==