

Technical Note

Trade Repository Enhancement for SWIFT WebAccess

1. Introduction

At present, Participants could access browser-based User Interface (UI) functions of Hong Kong Trade Repository Reporting (TR) system through secured SWIFTNet InterAct messaging service. The current SWIFTNet InterAct solution adopts conventional Java applet technology i.e. thin program module embedded in the user's web browser to handle user login between the web browser of users and TR system. As technology advances, mainstream web browsers, including Microsoft Internet Explorer, are no longer supporting Java applet technology. As a result, SWIFT will introduce a new SWIFT WebAccess solution to replace the SWIFTNet InterAct messaging service by year 2020.

To strengthen the authentication process, this new SWIFT WebAccess solution will adopt Security Assertion Markup Language (SAML), which is an open industrial standard for user authentication, and ride on a new SWIFT Identity Provider (IdP) platform under the central SWIFT infrastructure. As a result, user authentication will be delegated to SWIFT.

Accordingly, the TR application will be enhanced to accommodate the following changes to tie in with the introduction of the new SWIFT WebAccess solution by SWIFT:

- (a) Existing login process to TR system through InterAct messaging and Java Applet via SWIFT network will be replaced by Security Assertion Markup Language (SAML) messaging for communication among end users' web browsers, SWIFT's central application and TR application; and
- (b) Administrative functions, including configuration and supporting functions, will be enhanced to cater for SWIFT's new WebAccess service.

2. Changes in Login and Administrative Functions

2.1 Decommissioning of Support for SWIFT InterAct Messaging and Java Applet

For login function, existing electronic communication between TR web pages on end users' web browsers and HKICL's TR server application using SWIFT InterAct messaging and Java Applet will no longer be supported.

2.2 TR Login via SWIFTNet

Under the new SWIFTNet WebAccess platform, SWIFT's central authentication service will be responsible for the login authentication process. In gist, end users will log in to SWIFT software, SWIFT network as well as TR application using the unified SWIFT login interface and SWIFT user credentials.

2.2.1 TR Application Login through SWIFT WebAccess Login Web Page

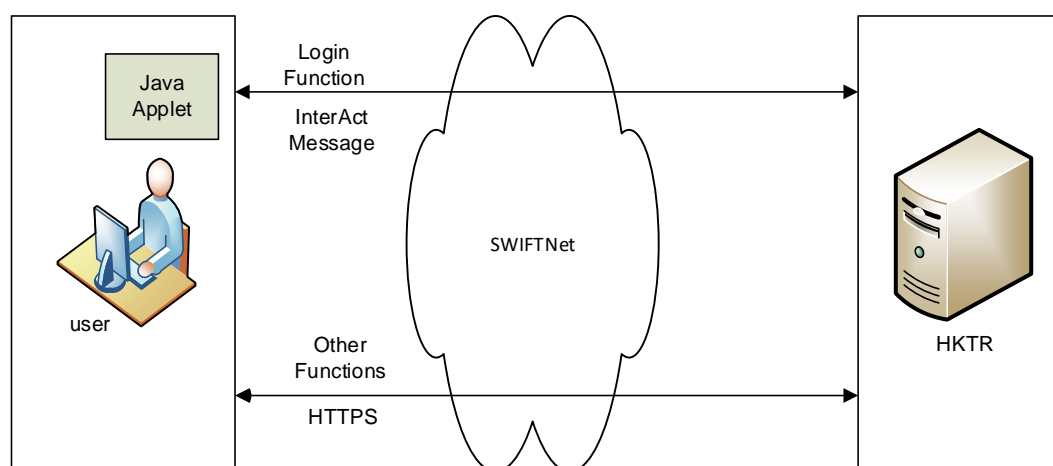
If a user logs in to TR application via the main page, a SWIFT WebAccess login web page rather than the existing TR application login interface will pop up for authentication purpose. After submission of the password associated with the SWIFT user, SWIFT will authenticate the user on behalf of TR application. If the authentication is successful, the SWIFT's user credential will be passed to TR application for identification purpose.

Since TR application identifies the user based on SWIFT's credential rather than TR's application user ID, association between SWIFT's user and TR's application user ID has to be established before first-time login to TR application. Please refer to Section 2.4 for the details of association.

Since both SWIFT WebAccess platform and TR application share the same login web page, there may be occasions where users may need to input credentials twice in order to log in to both SWIFT WebAccess and TR application after clicking the main page link.

2.2.2 Change of Underlying Electronic Data Exchange Format and Workflow

For access to UI functions via SWIFTNet, electronic data need to be exchanged through SWIFT's Browse and InterAct service. For normal data exchange between end users' web browsers and TR back-end application, SWIFT's Browse will be used based on HTTPS protocol, an industrial web browsing standard widely adopted in the Internet. For important data exchange like login to application, InterAct messaging service will be used as it adopts XML data format using small program called Java Applet. The different flows are illustrated as follows:

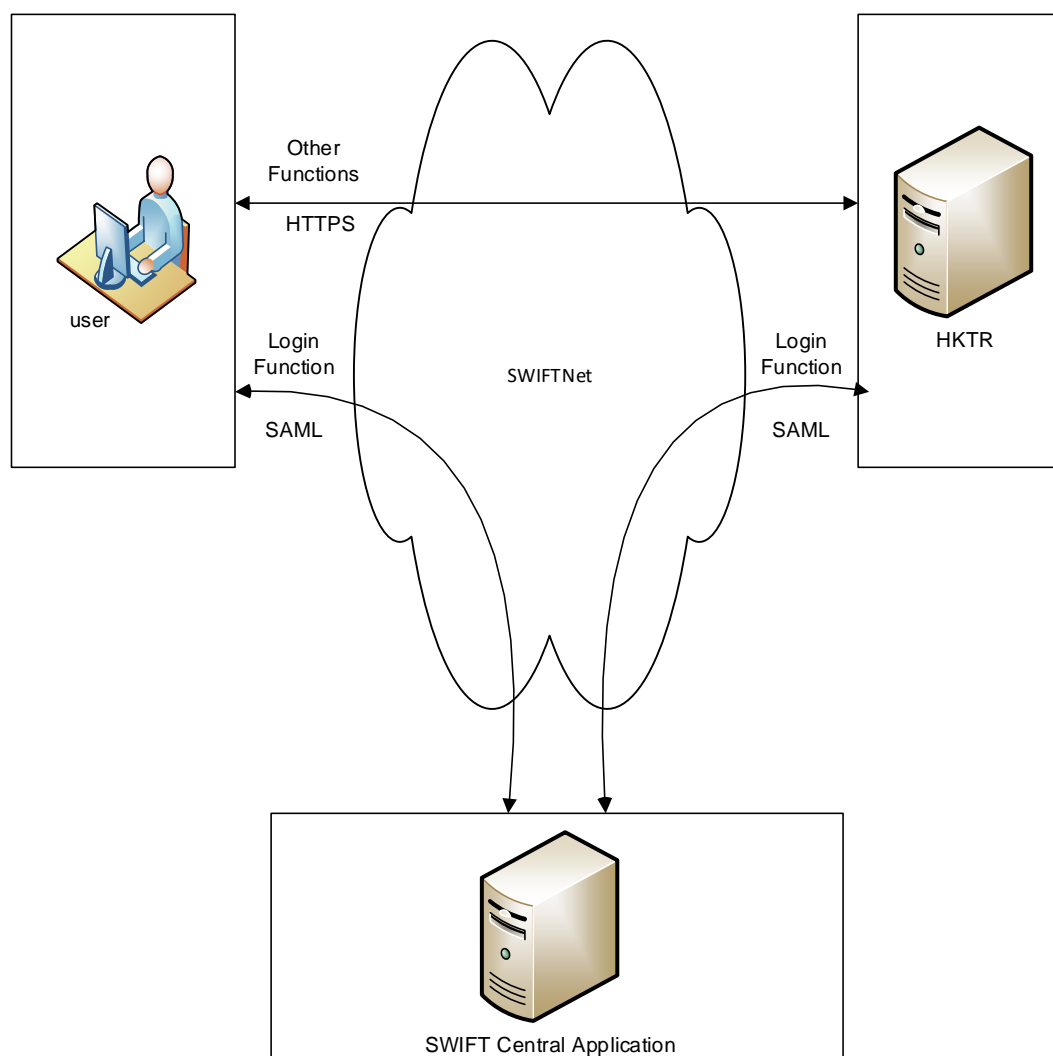


Note: InterAct Message will be decommissioned in 2020

As collaborating browser software of Microsoft Internet Explorer will no longer support Java Applet technology, the old SWIFTNet Browse service based on Java Applet will be replaced by the new revamped platform of SWIFT WebAccess in 2020.

The UI functions under the new platform, except for login function, will adopt the same HTTPS protocol for data exchange as the existing SWIFTNet Browse environment. The login function which relies on SWIFT's InterAct messaging and Java Applet will be replaced by new Security Assertion Markup Language (SAML) protocol, which is an open standard of authentication and authorization for data exchange. The underlying data exchange flow will also be changed to facilitate a more complicated 3-way communication among end user's web browser, SWIFT WebAccess central application and HKICL's TR application.

The new workflow is briefly illustrated as follows:



The user authentication (i.e., login function) will be delegated from TR application to SWIFT.

2.3 One Distinctive SWIFT User/Certificate for One TR Application User

Under the existing SWIFTNet Browse environment, TR system allows multiple TR application user accounts to associate with one user digital certificate issued by SWIFT.

To tighten security control, the new SWIFT WebAccess platform will no longer allow the sharing of one single SWIFT user certificate among multiple application users using TR application. Individual SWIFT users must have their own certificates in order to log in to the application systems.

2.4 SWIFT User Account Association and Disassociation

Following the transfer of user authentication function from TR application to SWIFT, the SWIFT's login screen instead of TR application's login screen will pop up when a user accesses the TR application web page.

In order for the user authentication function of SWIFT WebAccess to work, an association between the SWIFT's user and the TR application user profile must be established.

Under the current SWIFTNet Browse platform, every TR application user account has to register a distinguished name (DN) prior to the first-time login.

Instead of pre-registering a user profile by TR application, the new SWIFT WebAccess platform will use a unique identifier called "Name ID" generated by SWIFT to associate a SWIFT user with a TR application user. As the Name ID is not visible to users, an account association function will be required to link up the SWIFT user and the TR application user profile.

2.4.1 SWIFT User Account Association

After migrating to the SWIFT WebAccess platform, a new SWIFT User Account Association function will be created to associate SWIFT's users with individual TR application user profiles. When a SWIFT user logs in to TR system with SWIFT credentials, the new function will associate his/her current identity with TR's pre-defined application user profile. Therefore, participant ID, application user ID and application user password will be required in order to establish such association.

The function only applies to the first-time login and the user will not need to repeat the procedure for subsequent logins once the association between SWIFT's user and TR application user profile has been established.

However, newly added TR application user account will be needed to establish the association again.

The SWIFT user account association function is described in Section 2.9.6.

2.4.2 SWIFT User Account Disassociation

A new function will also be added to the TR application to remove the association between a SWIFT user and the associated TR application user profile.

The participant administrator can remove the SWIFT user account association using the Maintain User Account function. Once the association is removed, the account association screen will pop up when the SWIFT user login again.

The delete SWIFT user account association function is described in Section 2.9.42.4.2.

2.5 Single URL for Primary and Backup Sites

The existing design of TR system infrastructure supports active-standby resilience between primary and backup sites. In case of disaster or annual drill, SWIFT users need to switch their client side configurations to the correct web site addresses in URL as these are different for the primary and backup sites.

Under the new SWIFT WebAccess platform, end users can configure and use one web site URL to access the TR application without worrying whether the data traffic should be routed to primary or backup sites. This would enhance the transparency of site switching to end users.

2.6 Logout, Timeout and Forced Logout Behaviours in SWIFT WebAccess

When a user logs out during the browser session timeout, an alert message will pop up informing the user about the expiry of the user session. After the user has confirmed the notification, he/she will be logged out by the system and the TR login page will appear for the user to login again. The same system behaviours apply to all supporting channels of the TR application.

After migration to SWIFT WebAccess, the TR login page will not pop up from the SWIFTNet channel. Instead, a new screen with system messages will be displayed. Details of the System Message Screen are set out in Section 2.9.7.

For Internet channel, the existing behaviour remains unchanged i.e., the TR login page will pop up for users to re-login.

2.7 User Account Disabled Scenarios in SWIFT WebAccess

With an appropriate role allocation, a participant administrator has the ability to disable a user. If the user logs in to the system and is disabled by another user, an alert message will pop up notifying the user of the expiry of the user session. After confirming the notification, the user will be logged out by the system. The TR login page will pop up. The same system behaviours apply to all supporting channels of the TR application.

After the launch of SWIFT WebAccess, the TR login page will not pop up from SWIFTNet channel. Instead, a new screen with system messages will be displayed. Details of the System Message Screen are set out in Section 2.9.7.

For Internet channel, the existing behaviour remains unchanged i.e., the TR login page will be displayed.

2.8 Password Expired / Forced Change of Password Scenarios in SWIFT WebAccess

A user is not allowed to access any application function if his/her application user password has expired, or the user is forced to change the password by the

administrator. Access will be resumed after the password is changed. The same system behaviours apply to all supporting channels of the TR application.

After the launch of SWIFT WebAccess, the validity checking of application user password will be skipped when users log in through SWIFTNet channel. User is still able to access the application functions even if the password has expired.

For Internet channel, the existing behaviour remains unchanged.

2.9 Changes of Administrative Functions

The following administrative functions need to be enhanced as a result of the changes below:

- Deletion of pre-registration of participants, DN's in TR user profiles; and
- Addition of SWIFT user account association and disassociation as described in Section 2.4.

2.9.1 Add User Account

The “SWIFT User Details” section and the “Add DN” button will be removed from the Add User Account function.

When a new user is created based on details of another selected user using the Create Like function, the details of SWIFT User Account Association will not be carried forward to the new user profile. The association details, including the SWIFT user name and SWIFT user DN(s), will be saved in the application user profile upon completion of the SWIFT User Account Association process.

Please refer to Appendix A for the revised UI screen layouts.

2.9.2 View User Account

A new information tab of “SWIFT User Account Association” is created in the View User Account function to show the SWIFT user name and the corresponding DN of the SWIFT user in the SWIFT's user certificate.

The user-requested report “ADMU0001 – User List Details” will be updated to include information on “SWIFT User Account Association”.

Please refer to Appendix A for the revised UI screen layouts.

2.9.3 View User List

A new searching criterion “SWIFT User Name” will be added to the View User List function and will be shown in the searching result.

The online report “ADMV2302 – View User List” will be updated to include this new column.

Please refer to Appendix A for the revised UI screen layouts.

2.9.4 Maintain User Account

Similar to the View User Account function, the “SWIFT User Account Association” section in the Maintain User Account function contains information on association between SWIFT user and TR application user account.

The existing ADD DN function will become obsolete.

If a user wants to delete the association of a SWIFT user from an associated TR application user profile for whatever reason, he/she can use the new delete association checkbox in Maintain User Account function. A warning message will pop up requesting confirmation of the deletion. However, an association is not allowed to be deleted if the user is logging in to the TR application.

The SWIFT user account association will be deleted automatically if an application user has been deleted. If the user access method has changed to “Internet” only, user is forced to delete the SWIFT user account association in this UI function.

Please refer to Appendix A for the revised UI screen layouts.

2.9.5 Add Participant

The “SWIFT User DN” field and corresponding “Add DN” button in the “Default Administrator Configurations” section will be removed from the Add Participant function.

A new drop-down list box will be added to indicate the user access method of default administrators.

The above changes will also apply to the registration of Business Entity (BE) by TR Participants.

Please refer to Appendix A for the revised UI screen layouts.

2.9.6 SWIFT User Account Association Screen

This is a new function to associate current SWIFT users with TR's pre-defined application user profiles. The participant ID, application user ID and application user password will be used to activate such association.

Once an association between SWIFT's user credentials and TR application user profile is established, the SWIFT user DN(s) and the SWIFT user name in the SWIFT user certificate will be saved in the application user profile. Each SWIFT user can only be associated with a single application user profile.

This user association function will not be triggered in subsequent logins of the same user. However, if the association of SWIFT's user credentials is deleted from the

application user profile, this function will be automatically triggered again upon next login.

If the application user password has expired, the user account association can still be established as the checking for password expiry will not apply to this process.

The common failure cases of user account association are:

- The institution of the SAML response message does not match the browser SWIFT DN maintained by Participant Details function;
- The application user is associated with another SWIFT user;
- The application user account cannot be found;
- The application user account is disabled;
- The password of application user account is incorrect;
- The application user has no privilege on accessing TR application through SWIFTNet channel.
- The application user account is disabled after 3 unsuccessful attempts. The number of attempts is cumulative and applied to all channels (e.g., login failure via Internet channel).

The existing SWIFT user DN registered by a user will be removed during system migration and cannot be used for enquiry after the system launch. Existing user need to go through the SWIFT user account association process to access the TR application.

The activity of SWIFT user account association will be recorded in the event log of the system report “ADMD0001 – Administrative Functions Audit Trail Report”.

Please refer to Appendix A for the revised UI screen layouts.

2.9.7 System Message Screen

A new screen with system messages will pop up when users encounter the following scenarios while browsing through SWIFT WebAccess platform.

- Browser session timeout;
- Session conflict, the same user has logged in to another browser session;
- Forced logout;
- User account is disabled;
- Successful logout from the application;
- Rejected responses by SWIFT WebAccess e.g., invalid login to SWIFT WebAccess;
- Unable to show the TR welcome page after successful login to the SWIFT WebAccess due to application user account being disabled etc.

Users can press the “Close” button on the screen to close the application window. Users should login the SWIFT WebAccess again in order to access the HKTR through SWIFTNet channel.

Please refer to Appendix A for the revised UI screen layouts.

3. User Impact

3.1 Pre-processing of Unapproved Parameter Maintenance Before TR Migration

Pre-processing of the following items may be required before the migration of TR application. Any outstanding record pending approval will be automatically rejected during the migration.

- Create User
- Change User Details
- Add Participant
- Register Participant

3.2 Participant Preparation for SWIFT WebAccess Service

To access the new SWIFT WebAccess platform, users need to subscribe to the SWIFT WebAccess before the big-bang migration of TR application. The major tasks required by SWIFT are listed in Section 3.2.1 to 3.2.5.

3.2.1 New URL and Network Configuration

The URL of TR after migration to SWIFT WebAccess is different from that of the existing SWIFTNet Browse. The new URL of SWIFT WebAccess will be set out in the new version of Administration and Interface Development Guide (AIDG) to be published in due course.

Users may need to configure their networks and firewall settings to ensure they can access to the new URL.

As described in Section 2.5, users need to be aware of the single URL change.

3.2.2 Subscription to SWIFT WebAccess Service

Under the existing SWIFTNet Browse environment, a user can access TR and/or MT applications after subscribing to the single SWIFT service dedicated to HKICL.

Under the new SWIFT WebAccess platform, dedicated TR and RTGS service profiles are required for individual TR and MT applications. To this end, SWIFT will issue a letter to individual participants asking for instruction on future subscriptions to either of or both TR and MT application(s) in due course. SWIFT will follow these instructions to migrate the individual settings of participants in Browse service to future TR and/or RTGS WebAccess services. For details of the process, please refer to the presentation materials distributed at the SWIFT User Group Meeting on 14 May 2019¹ and SWIFT KB Tip 5021541. Users can also contact their SWIFT account managers for more information.

¹ At the SWIFT Hong Kong User Group Meeting on 14 May 2019, SWIFT Hong Kong announced the requirement for the WebAccess migration followed by distribution of PowerPoint materials, such as adjustment of monthly fee, new arrangement of PKI certificates and auto provisioning of the new SWIFT WebAccess services...etc. Any user who has missed the user group meeting and has not received the presentation materials from SWIFT, please contact Ms Debbie Lee of SWIFT (email: Debbie.lee@swift.com) or your SWIFT relationship manager at your earliest convenience.

3.2.3 SWIFT Role Based Access Control (RBAC) Assignment

TR application has its own role based access control functions over access rights of different TR users without using SWIFT's role-based access control (RBAC).

After migration to the new SWIFT WebAccess platform, SWIFT mandates the use of one single default role for all new SWIFT WebAccess service profiles of TR application. As such, the security officers of TR users should assign the SWIFT's default RBAC role to all the SWIFT user accounts in order to access the TR application.

3.2.4 Procurement of Additional SWIFT Certificate

As mentioned in Section 2.3, SWIFT WebAccess mandates the use of one single certificate for one user. All users who access SWIFT WebAccess should have dedicated SWIFT certificates. Sharing of SWIFT certificates is no longer supported by TR application.

Users currently share SWIFT user certificates may need to purchase additional certificates from SWIFT in order to comply with the future requirement of SWIFT WebAccess platform.

3.2.5 Configuration / Upgrade of SWIFT Software

Users should closely liaise with SWIFT on migration of on-premise items related to SWIFT software e.g., upgrade of SWIFT WebAccess GUI Package for Alliance Web Platform (AWP).

Individual participants may need to undertake additional migration tasks for subscription to SWIFT WebAccess according to their SWIFT settings. For more thorough and detailed descriptions of these tasks, TR SWIFT participants should attend SWIFT's briefing sessions and refer to SWIFT's manuals and training materials.

3.3 SWIFTNet FileAct Channel

There is no impact on Straight-through Processing (STP) channels for submission of report/data since the SWIFT WebAccess migration only affects web browsing via SWIFTNet channel.

3.4 Local Terminal Service

There will be no impact on the Local Terminal Service provided by HKICL as user authentication will be done by TR user interface as usual.

4. Migration

The SWIFT WebAccess service migration is not an enhancement initiative. This migration involves significant changes in client setting/configuration of users, SWIFT's WebAccess central application and HKICL's TR server application.

Collaboration among all parties is required to ensure the migration is done in a progressive and orderly manner. According to the latest discussion with SWIFT, a phased approach will be adopted for the migration with the major tasks set out in the ensuing Sections 4.1 to 4.5. The tentative schedules will be provided in the circular associated with this technical notes document.

4.1 Setup of New SWIFT WebAccess Service Dedicated to TR Application

This is the first major task to be performed by SWIFT before proceeding with other migration tasks. SWIFT is responsible for setting up the new SWIFT WebAccess service for TR application and another new service for RTGS. To alleviate the burden of existing participants to subscribe to the new TR service, automatic re-provisioning will be adopted by SWIFT.

As per the description in Section 2.2.2, the existing RTGS Browse service will become two (2) distinctive TR and RTGS WebAccess services. Before launching the new service, SWIFT will send letters to seek users' agreement on the automatic re-provisioning of the new SWIFT WebAccess services in due course. For users who only need to access TR application via future SWIFT WebAccess service, they should request for SWIFT auto-provisioning to TR WebAccess service only. Otherwise, users will be automatically re-provisioned to the new RTGS WebAccess service as well, which may incur additional service charges.

After the WebAccess service is created by SWIFT, it can be present in parallel with the existing Browse service without affecting participants' continuous access to TR's GUI function via Browse service.

4.2 Participant Setup

Following the user group meeting held by SWIFT on 14 May 2019 by SWIFT, participants should begin planning their setups.

According to information provided by SWIFT, participant setup includes certificate setup, role assignment, update of SWIFT software etc. For full details of participant setup, please refer to SWIFT KB Tip 5021541 or contact your SWIFT account manager.

The setup can only be started after launching of the WebAccess service by SWIFT as described in the previous section. End-to-End test cannot be conducted at this stage until HKICL has completed the setup as described in the following section.

4.3 Connectivity Test by Participants

To streamline the migration of TR application, an end-to-end connectivity test will be conducted with participants in the weekends before the launch date. This test aims to verify the propriety of participants' setups and SWIFT's setup for the new SWIFT WebAccess service of TR application (please refer to Sections 4.2 and 4.1 respectively) and provide an opportunity for participants to identify any configuration issue at an earlier stage.

HKICL will release a temporary web page in TR application server in due course. Successful access to the web page implies that the major configurations of SWIFT WebAccess (described in Section 4.2) and connection between participants and SWIFT are correct. It will also help verify the accessibility of participants' network/firewall settings to HKICL TR application servers via SWIFT's network based on new SWIFT WebAccess service albeit login via SWIFT WebAccess service cannot be done at this stage.

4.4 TR Application Migration

A big-bang approach will be adopted for the migration of TR application to SWIFT WebAccess workflow and interface in the migration weekends, after which end users can only log in via SWIFT WebAccess service with the new URL.

4.5 Post-implementation Verification

After the final migration as described in the previous section, the HKMA will invite some participants to participate in the post-implementation verification in the same migration weekends. Participants concerned should ask their major users to log in to the TR application and complete the SWIFT user account association (please refer to Section 2.4.1) for the first time.

~ End ~