



Change of Authentication Arrangement of CCASS Terminal Access

Information Package for HKSCC Participants and Designated Banks

Issue Date: December 2022

Modification History

Version	Date	Modified By	Synopsis
1.0	Oct 2022	HKSCC	First draft
2.0	Dec 2022	HKSCC	Updated the following: <ul style="list-style-type: none">• Section 2.2 & 3.1 – added details on email registration• Appendix A – supplemented with screenshots on email registration procedure

Latest updates are highlighted in orange.

Contents

1. Introduction	4
2. Overview of the Change of Authentication Method	4
2.1. Objective	4
2.2. Migration from Smartcard to 2FA	4
2.3. Tentative Timeline	5
3. Operational Changes during Migration	5
3.1. Pre-parallel Run – Email Registration	7
3.2. Commencement of Parallel Run	8
3.2.1 Preparation Work as a DA	9
3.2.2 Preparation work as a user	9
3.2.3 Smartcard and smartcard reader maintenance	9
3.3. End of parallel run	9
4. Important Notes	10
4.1. Arrangement for CPs that have Appointed Settlement Agent	10
4.2. User Creation	10
4.3. Assign Business User Groups for DAs	11
4.4. Disposal Handling of Smartcard and Smartcard Reader	11
4.5. Separate User Account in Mobile Application	11
4.6. Obsolescence of Existing eService and Introduction of New eService	12
5. Contact Information	12
6. Checklist	12
Appendix A. Email registration procedure for users	13
Appendix B. 2FA Login Procedure	18

1. Introduction

As set out in the circular dated 1 September 2022 (Reference: [CD/OES/CCASS/032/2022](#)) and 31 October 2022 (Reference: [CD/OES/CCASS/038/2022](#)), to enhance the security assurance and in line with the authentication arrangement of VaR Platform, CCASS Participants¹ (CPs) and HKSCC Designated Banks (DBs)² will progressively migrate to logging into CCASS Terminal by Two-Factor Authentication (2FA) replacing the existing authentication method with smartcard and smartcard reader. The 2FA includes a regular password together with an One-Time-Password (OTP) generated by soft token via mobile application or email. To ensure a smooth transition, a parallel run for both authentication methods will be provided to CPs and DBs switching from smartcard to 2FA.

This Information Package aims to provide detailed information to assist CPs and DBs to prepare and do necessary setup ahead of the commencement of parallel run. Further information will be provided in this Information Package on the migration progress from smartcard to 2FA, CPs and DBs will be notified via circular for information updates.

2. Overview of the Change of Authentication Method

2.1. Objective

In existing practice, a CCASS user must insert his/ her smartcard into the smartcard reader connecting to a CCASS Terminal and input a correct smartcard PIN to logon to CCASS Terminal. In order to enhance security assurance, HKEX is planning to replace the existing authentication method by 2FA, which means that users of CPs and DBs can logon to CCASS Terminal using a regular password together with an OTP generated by soft token via mobile application or email, instead of smartcard. Same technology is in place for VaR Online, hence, the login experience should be similar for the existing VaR Online users.

2.2. Migration from Smartcard to 2FA

In order to ensure a smooth transition switching from smartcard to 2FA, HKEX will provide CPs and DBs an approximate 2-month parallel run period of both authentication methods. During the parallel-run, users are allowed to access to CCASS Terminal with either smartcard or 2FA, and are encouraged to start accessing CCASS Terminal with 2FA. Upon the end of parallel run, 2FA will be the sole authentication method to access CCASS Terminal.

¹ CCASS Participants includes Clearing Participants, Custodian Participants, Stock Pledgee Participants, Clearing Agency Participants of HKSCC.

² HKSCC CPs and DBs who access to CCASS through Participant Gateway (PG) will not be impacted in this exercise, further planning of the authentication arrangement of PG will be announced in due course.

For the preparation of using 2FA, CPs and DBs should register the designated email address of users, regardless of obtaining the OTP via mobile application or email.

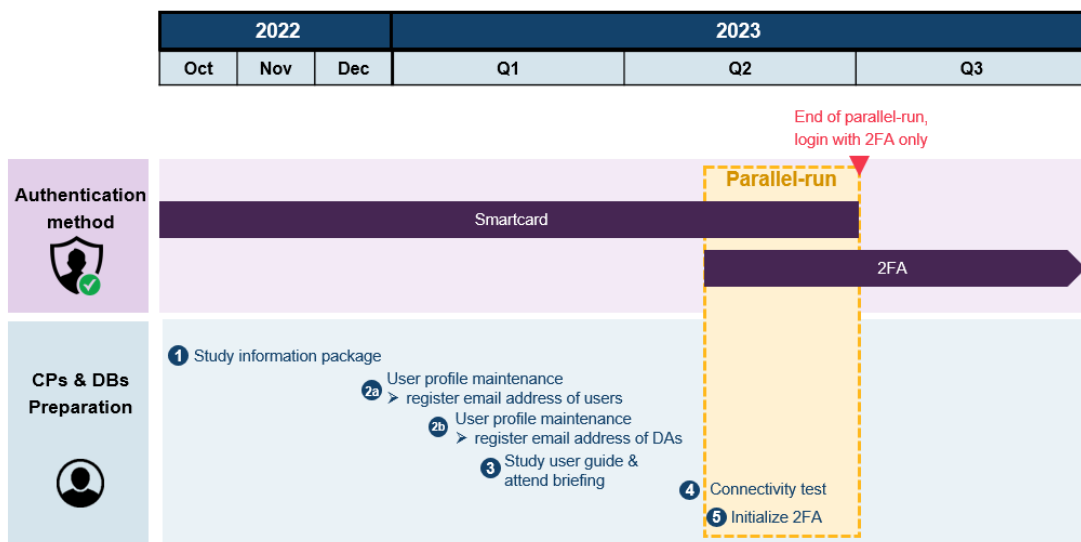
The purpose of the email address registration is for users to obtain OTP as an authentication to setup their regular password. Upon the completion of regular password setup, users can change their setting to obtain OTP via mobile application, or remain in email based on their preferences. For security reasons, HKEX recommends users to make use of mobile application to obtain OTP.

It is strongly recommended to take action to register email address for users as soon as possible, otherwise, users would not be able to receive OTP for authentication during the first time 2FA login. Furthermore, user profile(s) without email address(es) registered will be obsoleted upon the end of parallel run.

A connectivity test will be arranged to verify the access to CCASS Terminal with smartcard before the start of parallel run. HKEX will also release user guide and arrange briefing to provide more information of the parallel run and the points to note.

2.3. Tentative Timeline

A summary of the upcoming activities and tentative schedule is shown below for reference:



CPs and DBs should follow the timeline to prepare for the implementation of 2FA accordingly. All CPs and DBs are encouraged to participate to access to CCASS Terminal with the new authentication method during the parallel run.

3. Operational Changes during Migration

There are changes to be applied on DMS throughout the parallel run to facilitate CPs and DBs to update and manage their users under the new authentication method.

To simplify the migration arrangement, Delegated Administrators (DAs) who perform the user profile maintenance functions and users will continue using the same set of user ID to access CCASS. In case users are not aware of their User ID, DAs can locate the User ID of their users through CCASS Function – User Profile Listing, please refer to the detailed procedure listed in [Appendix A](#). No special attention is required for DA to take note of, the format of the User ID for DAs and users across the Clearing House is shown as follows:

User Type	CPs	DBs
User ID for DAs <i>(to be assigned by HKEX)</i>	Participant ID + X/Y/Z + 1-9, e.g. B01234X1	Participant ID + X/Y/Z + 1-9, e.g. BNK999X1
User ID for Users <i>(existing users were assigned by HKEX, new users to be assigned by DAs upon the parallel run)</i>	Participant ID + 2 custom alphanumeric e.g. B0123401	Participant ID + 2 custom alphanumeric e.g. BNK99901

2FA includes a regular password together with an OTP, which is generated by soft token via mobile application or email. Upon the password setup, users can choose to obtain the OTP via mobile application or email during the first time 2FA login and they can change the channel to receive OTP in their profile settings afterwards.

To receive OTP via mobile application, users can register their accounts on the ForgeRock Authenticator App. The App can be downloaded from [Google Playstore](#) for Android users and [Apple App Store](#) for iOS users. If users are existing VaR Online users and using mobile application to receive OTP, a separate account should be registered in ForgeRock Authenticator App. The registered accounts in ForgeRock Authentication App can be distinguished by user IDs. Users should refer to [Appendix B](#) for the registration procedure.

If users choose to receive OTP via email, the OTP will be sent to their registered email addresses in DMS. If users would like to update the registered email addresses, they shall request their DAs to perform the user profile update in DMS, which shall be effective shortly upon the completion of maker-checker process.

The following diagram is an illustration of the overall operational changes and the related tasks for DAs and users at different stage, and the details will be covered in the following sections:

Change of Authentication Arrangement of CCASS Terminal Access Information Package for HKSCC CPs and DBs

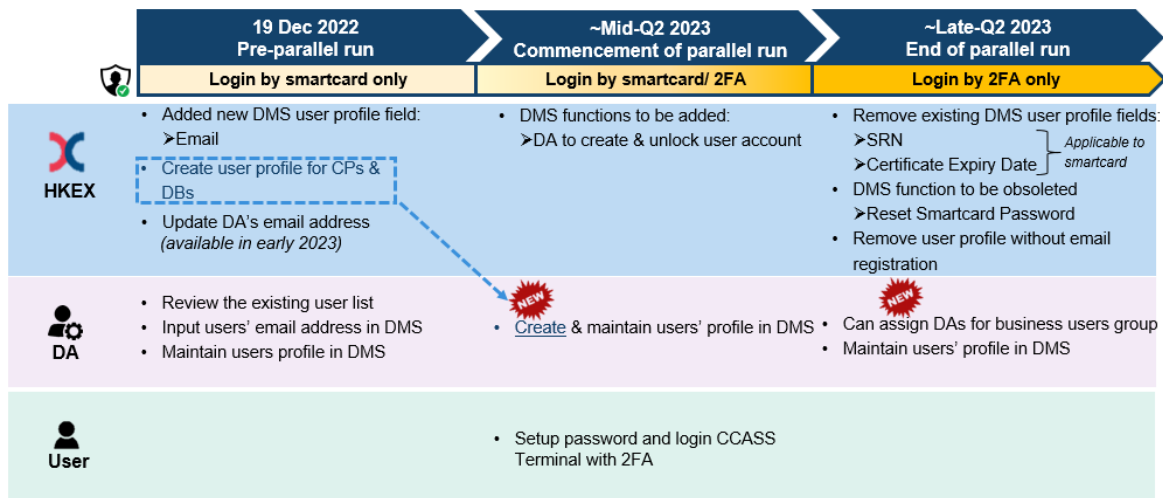


Table below summarised the changes in terms of user profile maintenance:

	Pre-Parallel Run		Parallel Run		End of Parallel Run	
	HKEX	DA	HKEX	DA	HKEX	DA
DA User Profile						
Creation	✓		✓		✓	
Profile maintenance	✓		✓		✓	
Email address registration	To be announced		To be announced		To be announced	
Deletion	✓		✓		✓	
Add business user group functions					✓	✓
User Profile						
Creation	✓			✓		✓
Profile Maintenance		✓		✓		✓
Email address registration		✓		✓		✓
Deletion		✓		✓		✓
Add DA group functions					✓	

Table 1: Summary of user profile maintenance

3.1. Pre-parallel Run – Email Registration

Starting from 19 December 2022, a newly added field “Email” will be available under the User Profile section in DMS to facilitate CPs and DBs to register users’ email addresses for 2FA. DAs shall register email address for their users so that they can receive OTP for authentication during the password setup when they login to CCASS Terminal by 2FA at the first time.

Sample screenshot of User Profile section in DMS as below:

Change User Profile - Detail

This is an end-user profile

User ID	B0123401
User Status	<input checked="" type="radio"/> ENABLED <input type="radio"/> DISABLED
Surname	TAI MAN
Other names	CHAN
Email	abc@abc.com.hk
Enable from	01-Jan-03 DD-MMM-YY
Disable after	DD-MMM-YY
Clearing House Options	Cash

DAs should review the existing user list and to proceed email registration for those active users who need migration to 2FA. DAs should input the designated email address(es) for their users in the “Email” field under User Profile section. For security reason, HKEX recommends all users to make use of emails with corporate domains to receive OTP. In addition, individual email address is recommended given the OTP is served as an authentication for individual to access CCASS Terminal, but, same email address can be registered in multiple user profiles to facilitate the operational need. **DAs are advised to focus on updating the email address of their users before the start of parallel run. It is not necessary to register the email address of DAs for the time being and their registration will be kicked off in early 2023.**

The email registration in DMS will require maker-checker mechanism, the email address will be updated and reflected in the user profile shortly upon the completion of maker-checker process. DAs who are assigned with User Access Level Code “EE” for Security Management Functions can then review the updated user profile via the DMS function – User Profile Listing. CPs and DBs should note that the new field “Email” will be displayed in the DA’s user profile as well, however such field is not editable by DAs.

If there is no email registered in the user profile, such user would not be able to receive OTP as an authentication for the password setup. In addition, such user profile will be obsoleted upon the end of parallel run.

For those inactive users, DAs should remove such users in DMS.

For the detailed procedure of email registration, please refer to [Appendix A](#).

3.2. Commencement of Parallel Run

The parallel run will commence in Q2 2023 tentatively. For users who have completed email registration, can start logging into CCASS Terminal with 2FA following the procedure indicated in [Appendix B](#) to verify the access using new authentication method, and are encouraged to use 2FA during the parallel run; while Smartcard access can be a backup login arrangement.

Existing user profile maintenance for DAs and users as of the commencement of parallel run will remain as is in CCASS, except DAs can start to create users with reference to [Table 1](#).

The newly created users shall use 2FA as the authentication method to access CCASS Terminal. Upon the end of parallel run, DAs could consider to assign the business user group functions to existing DAs by themselves or add DA group functions to existing/newly created users via eService DA 3 – CCASS/ CCMS Terminal Delegated Administrator Application/ Maintenance Form, DAs shall review the user list and delete the account that is no longer needed in DMS after the function is assigned to the respective account.

3.2.1 Preparation Work as a DA

Update in DA functions

During the parallel run, DAs can opt to access DMS with either smartcard or 2FA authentication, preferably 2FA, whereas, the login procedure shall be similar to users as indicated in [Appendix B](#). Besides, DAs will be responsible for creating user via DMS, which was done by HKEX previously. While smartcard PIN reset for DA is still responsible by HKEX, DA is responsible for unlocking and deleting user during the parallel run. The user guide with details of DA functions will be available in due course.

The newly created users during the parallel run period shall access to CCASS Terminal by 2FA only.

3.2.2 Preparation work as a user

Upon the email address registered in DMS by DAs, users shall setup his/her password following the procedure as listed in [Appendix B](#).

3.2.3 Smartcard and smartcard reader maintenance

CPs and DBs could submit the maintenance request via eService SCard 1 – Smartcard Maintenance for User and DA in [Client Connect](#), only for DA password reset. However, smartcard and smartcard reader will not be available for purchase upon the commencement of parallel run.

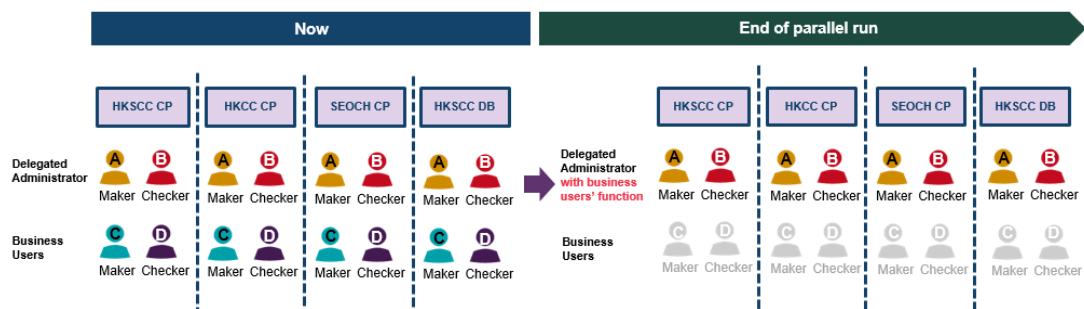
3.3. End of parallel run

Parallel run will end in around 2-month timeframe. All users are expected to have completed login to CCASS Terminal via 2FA by then, and should continue to access by 2FA going forward. 2FA will be the sole authentication method to access CCASS Terminal since the time; smartcard authentication method will be obsolete. Moreover, the following fields from User Profile section in DMS will be removed per the obsolescence of smartcard:

- a) SRN
- b) Certificate Expiry Date

Update in DA user role

Nowadays, DA and business user are maintained as separate user profile. Upon the end of parallel run, like VaR Online, DAs can also be assigned with business user groups, as such they can access to both DA's and Business User's functions using the same user ID. DA shall delete the user accounts, after the respective business user functions have been assigned to the DA user profile. An illustration of the user ID allocation of multiple entities is indicated in the following diagram:



For those users who have yet to complete email registration in DMS upon the end of parallel run, their account and profile will be removed, and DAs have to re-create the user profiles if deemed necessary.

eService DA 3 – CCASS/ CCMS Terminal Delegated Administrator Application/ Maintenance Form shall be submitted for the DA user profile maintenance such as email address.

4. Important Notes

4.1. Arrangement for CPs that have Appointed Settlement Agent

The login arrangement for Settlement Agent remains unchanged. For CPs (the principals) that have appointed settlement agent to access CCASS and conduct settlement, should perform email update in DMS for the users of settlement agent.

4.2. User Creation

CP and DB should base on its operational needs to maintain the number of users required, and should remove the inactive accounts that are not required anymore.

4.3. Assign Business User Groups for DAs

As mentioned in [section 3](#), DAs can be assigned with business user functions upon the end of parallel run. For those who currently possess 2 sets of user ID (e.g. B01234X1 and B0123401) to access DA and business user functions respectively, can follow the below procedure to assign business user groups to his/ her DA profile. Below procedures should be executed:

1. Pre-parallel run:
 - Update email address in both DA and business user (B01234X1 and B0123401) profile respectively
2. Commencement of Parallel Run:
 - Access CCASS Terminal for DA and users functions via the user ID B01234X1 and B0123401 respectively by 2FA or smartcards, preferably 2FA
3. End of Parallel Run:
 - DA assigns business user groups to B01234X1 profile and DA removes the profile B0123401
 - User holding B01234X1 can access both DA and business user function via 2FA

4.4. Disposal Handling of Smartcard and Smartcard Reader

Upon the end of parallel run, all smartcards and smartcard readers will no longer be in use for accessing to CCASS Terminal. CPs and DBs should also consider the necessity of purchasing smartcard reader and smartcard prior to parallel run period to avoid wastage. Users who have tested and confirmed that they can access CCASS Terminal with 2FA, shall dispose the smartcards and smartcard readers by their own means at the end of the parallel run, HKEX takes no responsibility or liability to the further usage of smartcard upon the end of parallel run.

4.5. Separate User Account in Mobile Application

Once users have registered the soft token profile in their mobile application, a new user profile with their CCASS user ID will be shown under “My Accounts”, users should obtain OTP from such profile when accessing to CCASS Terminal. Meanwhile, CPs and DBs should note that users have to register separate soft token profiles and obtain OTP from respective profile to access CCASS Terminal and VaR Online (applicable to CPs only).

4.6. Obsolescence of Existing eService and Introduction of New eService

One of the eServices relating to smartcard maintenance (i.e. SCard 1 - Smartcard Maintenance for User and DA) currently available in [Client Connect](#) will be obsoleted upon the end of parallel run. A new eService (i.e. DA 3 – CCASS/ CCMS Terminal Delegated Administrator Application/ Maintenance Form) will be available upon the commencement of parallel run to maintain DAs' profile, DA can maintain their user profile through such eService by then.

5. Contact Information

For any enquiries about the change of authentication method of CCASS Terminal access, please contact CCASS Hotline or Email indicated below:

- CCASS Hotline: +852 2979 7111 during normal office hours from 09:00 to 18:00 (Mondays to Fridays, excluding public holidays)
- CCASS Email: ClearingPS@hkex.com.hk

6. Checklist

ITEMS TO BE CHECKED		✓
1	To read and understand this document	
2	To coordinate with internal IT teams and/or system vendors for necessary preparation before the start of parallel run	
3	To understand the timeline for the migration from smartcard to 2FA	
4	To understand the timeline and procedure for email registration and accessing to CCASS Terminal via 2FA	
5	To understand the changes in DA profile and Business User management	
6	To understand that smartcard will be obsoleted upon the end of parallel run	
7	To review the existing accounts for email registration	

Appendix A. Email registration procedure for users

For checking User ID (to be perform by DA Maker or DA Checker)

#	Process	Sample screenshot
1	Access to DMS via https://www.cass.com/dms	
2	Navigate to the View Listings tab and then click User Profile Listing ³ tab from the menu bar	
3	The profile of all their users including DA will be displayed. DA can locate the respective User ID which is associated with the user name.	

³ The User Profile Listing function time in CCASS is 07:00 to 19:00 on Mondays to Fridays, and 09:00 to 13:00 on Saturdays, except for public holidays.

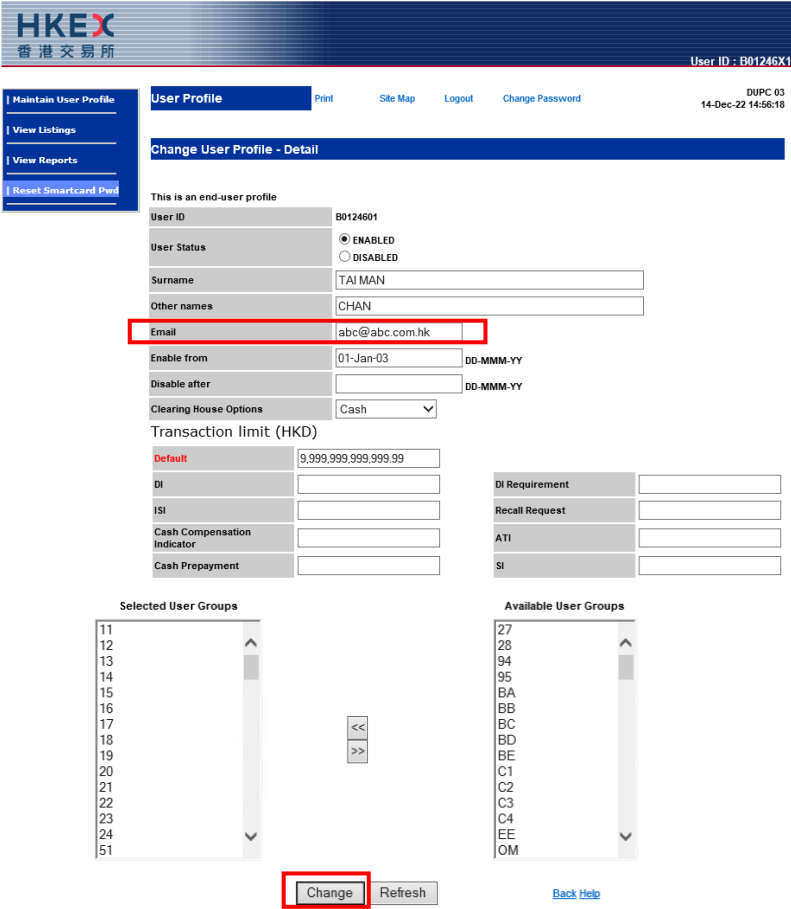
Change of Authentication Arrangement of CCASS Terminal Access
Information Package for HKSCC CPs and DBs

For submitting request (to be performed by DA Maker)

#	Process	Sample screenshot
1	Access to DMS via https://www.ccass.com/dms	
2	After locating the User ID, navigate to Maintain User Profile tab and then click Change User Profile ⁴ tab from the menu bar	
3	Search user by entering "User ID" and click Submit	

⁴ The Change User Profile function time in CCASS is 07:00 to 19:00 on Mondays to Fridays, and 09:00 to 13:00 on Saturdays, except for public holidays.

Change of Authentication Arrangement of CCASS Terminal Access Information Package for HKSCC CPs and DBs

#	Process	Sample screenshot
4	The detailed user profile will be displayed, update user's email address in "Email" field, and click Change	 <p>The screenshot shows the 'Change User Profile - Detail' page for an end-user profile. The 'Email' field is highlighted with a red box. The 'Change' button at the bottom is also highlighted with a red box. The page includes a navigation menu on the left, a header with the HKEX logo and user ID, and various form fields for user details and transaction limits.</p>

Change of Authentication Arrangement of CCASS Terminal Access Information Package for HKSCC CPs and DBs

For authorizing request (to be performed by DA Checker)

#	Process	Sample screenshot
1	On the same screen of submitting request performed by DA Maker, review and execute the request by entering "Checker ID" and "Authorization Code ⁵ ", then click Confirm	
2	The change of user profile is completed with message "The above user profile is changed successfully". The change of user profile shall be effective shortly after.	

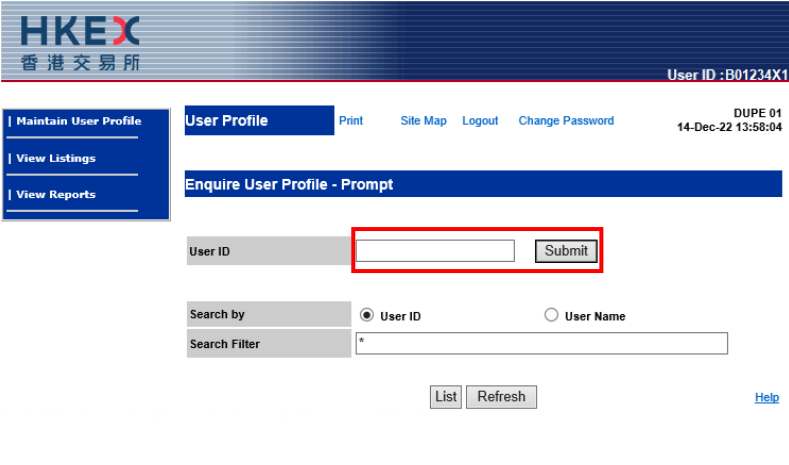
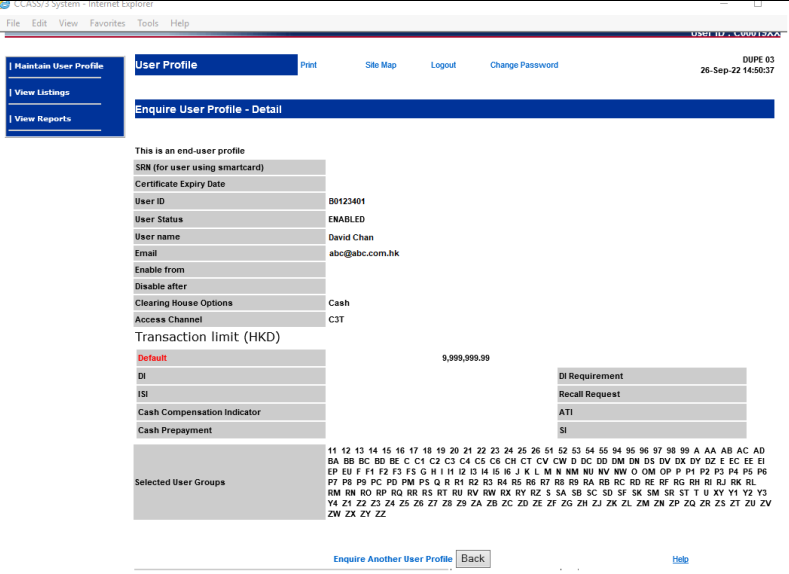
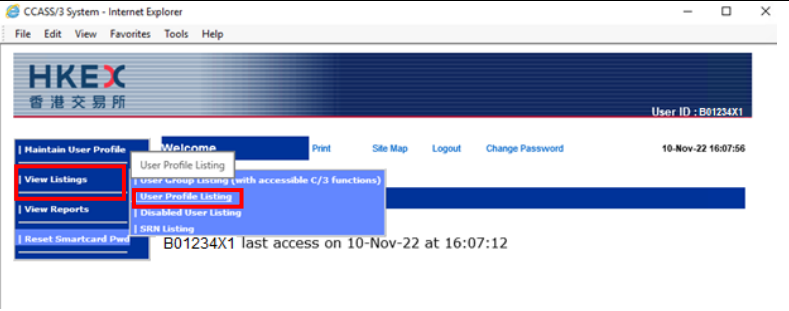
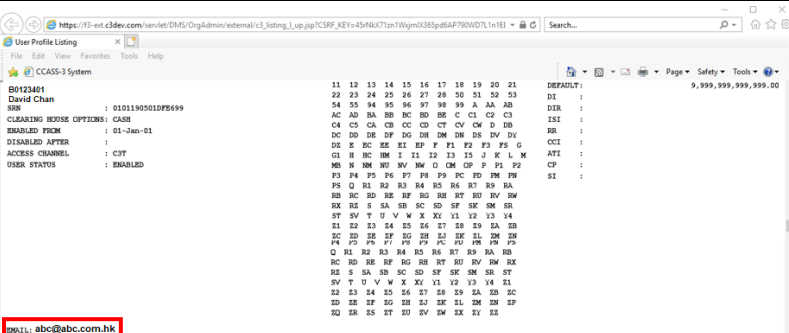
If there are multiple users that are required to update, DAs maker and checker have to repeat the above steps to submit and authorize the change of user profile request for each user.

For user profile listing download (to be performed by DA Maker or DA Checker)

#	Process	Sample screenshot
1	To review the updated user profile, navigate to Maintain User Profile tab, then click Enquire User Profile	

⁵ DA Checker's Authorization Code can be obtained from the CCASS function - Get Authorisation Code. The Authorisation code will be renewed at the beginning of each month.



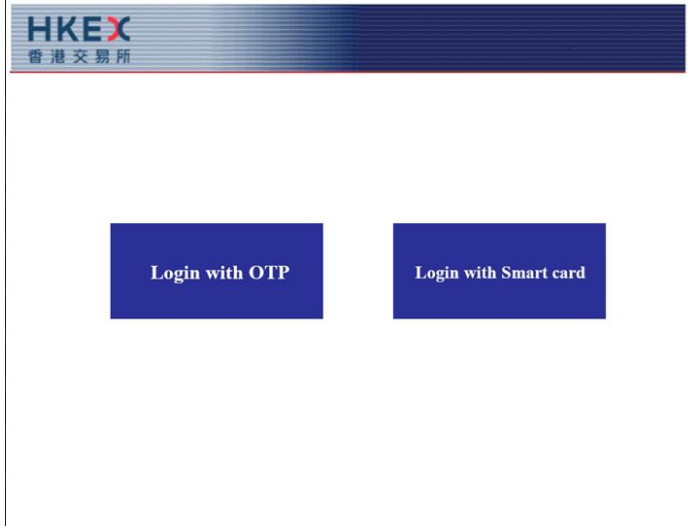
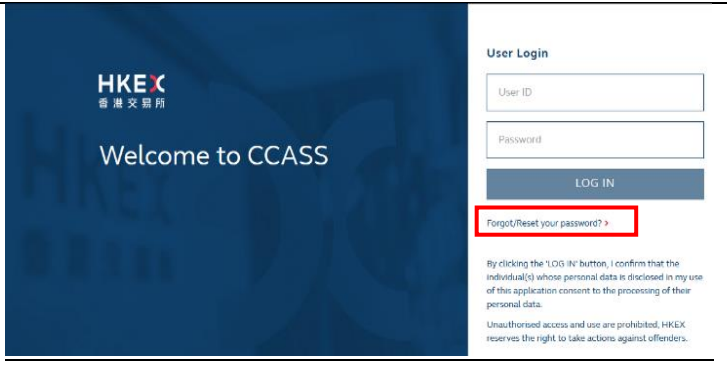
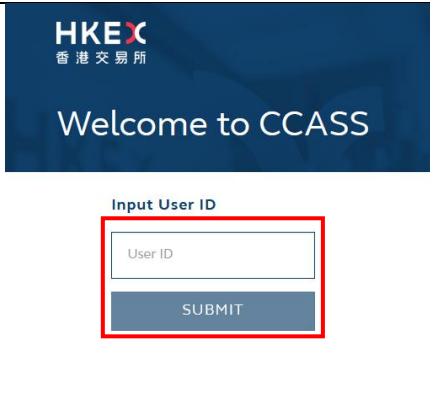
Change of Authentication Arrangement of CCASS Terminal Access Information Package for HKSCC CPs and DBs

#	Process	Sample screenshot
2	Enter the User ID and click Submit	
3	The detailed user profile will be displayed	
4	For DAs who want to download the latest user profile listing, can navigate to the View Listings tab and then click User Profile Listing ⁶ tab from the menu bar	
5	The User Profile Listing with User ID, registered email address and the user account details will be generated	

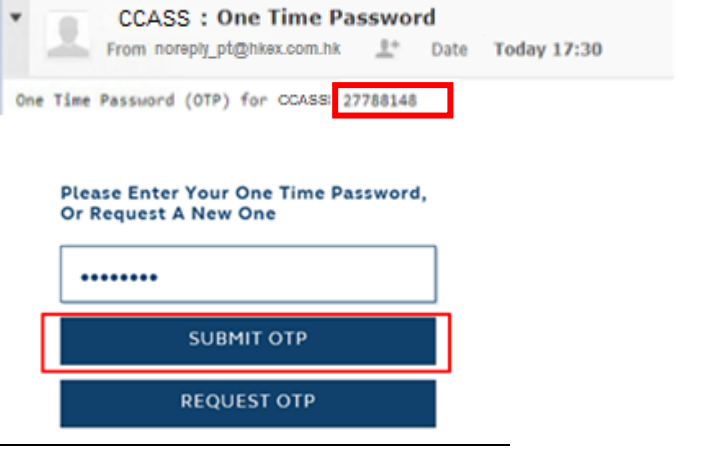
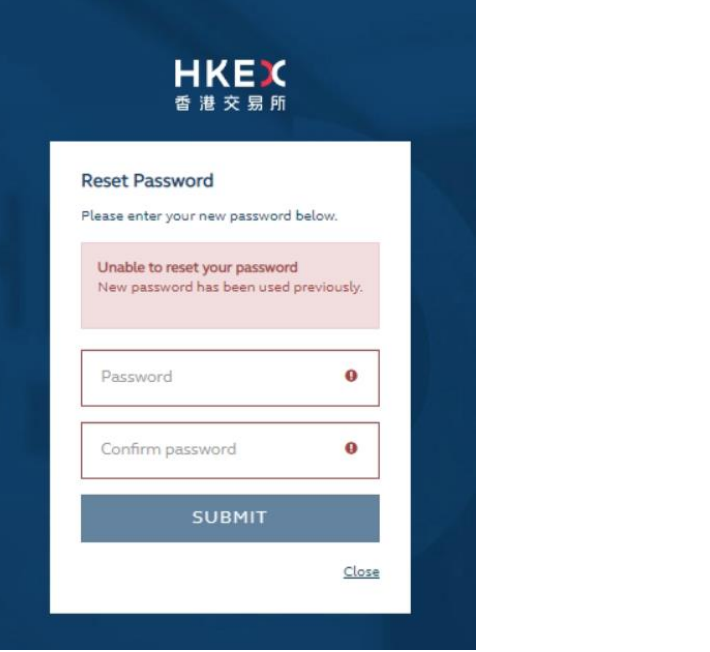
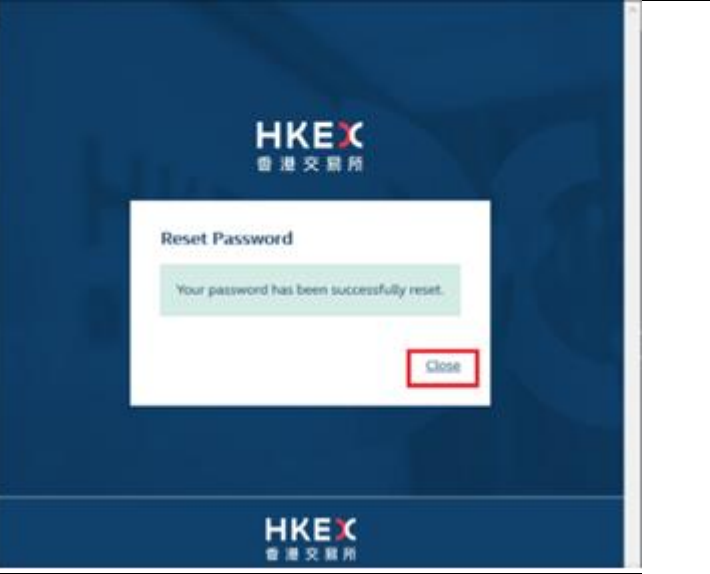
⁶ The User Profile Listing function time in CCASS is 07:00 to 19:00 on Mondays to Fridays, and 09:00 to 13:00 on Saturdays, except for public holidays.

Appendix B. 2FA Login Procedure

First Time Login

#	Process	Sample Screenshot
1	DA access to DMS via https://www.ccass.com/dms / User access to CCASS Terminal via https://www.ccass.com/	<p>For DA:</p>  <p>For User:</p> 
2	During the parallel run, users can select the appropriate login method, user to click the appropriate button and proceed	
3	Users to click "Forgot/Reset your Password" button on the login page	
4	A pop-up window will be displayed, user input their User ID and clicks "SUBMIT" button	




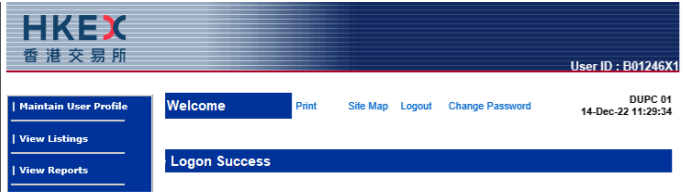
Change of Authentication Arrangement of CCASS Terminal Access
Information Package for HKSCC CPs and DBs

#	Process	Sample Screenshot
5	User receives OTP in their registered email which is valid for 5 minutes, user input the email OTP back in the pop up window	
6	User input new password twice to complete the setup of their password	
7	Confirmation of successful password reset will be displayed, user clicks "Close" to close the reset password window and return to the previously opened login page	

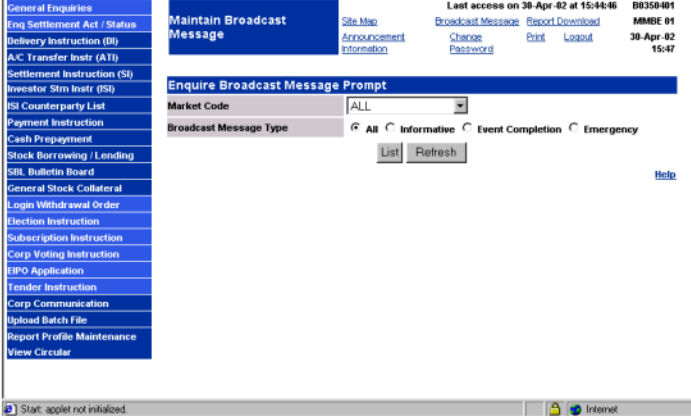
Change of Authentication Arrangement of CCASS Terminal Access
Information Package for HKSCC CPs and DBs

#	Process	Sample Screenshot
8	User input the User ID and the newly set password, and clicks "LOG IN"	
9	The system will ask user to register the mobile devices for the 2FA. User clicks "REGISTER DEVICE"	
10	User to search "ForgeRock Authenticator" from Google Play or Apple's App Store If users have been using ForgeRock Authenticator for VaR Online's logon, it is not necessary to download the same App again, and can skip this step.	
11	User can open the "ForgeRock Authenticator" mobile app, and click + sign to scan the QR code, then click "LOGIN USING VERIFICATION CODE" in the browser to continue.	
12	User to click the account from mobile app and then click to generate a OTP	



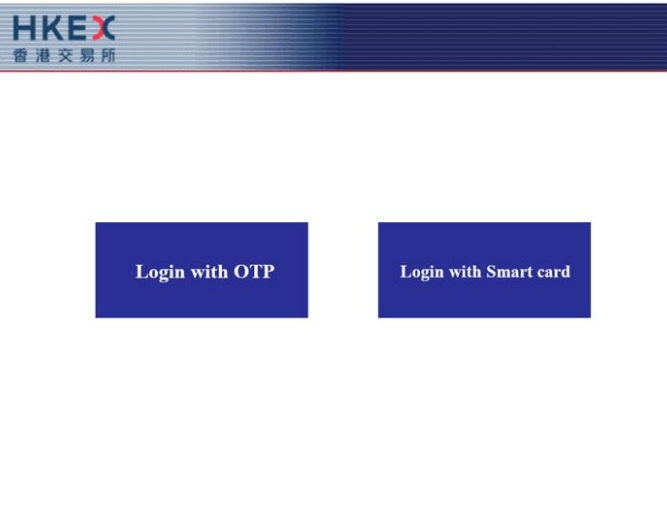
Change of Authentication Arrangement of CCASS Terminal Access
Information Package for HKSCC CPs and DBs

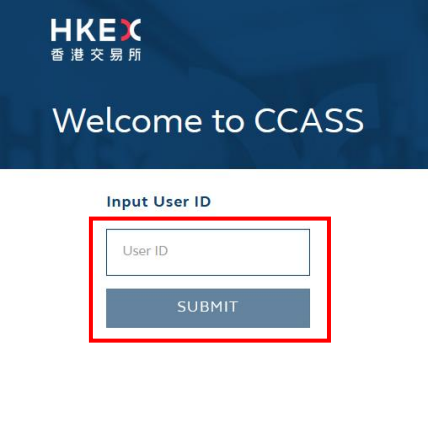
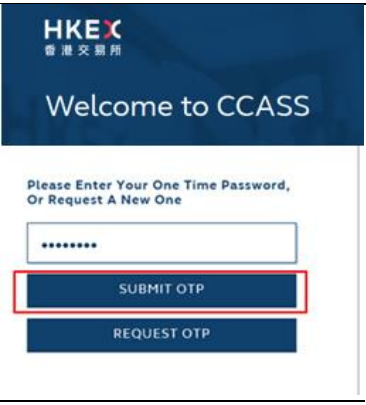
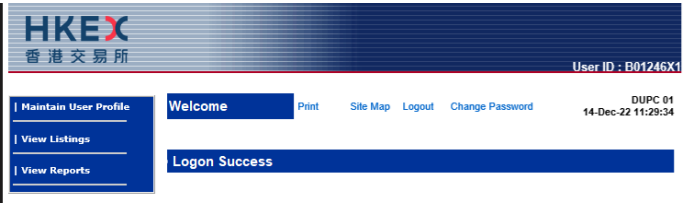
#	Process	Sample Screenshot
13	<p>If user wish to receive OTP via their registered email, he/she can click the “SKIP THIS STEP” button to opt-out the mobile app OTP. A message will be displayed to warn user about the risk of using Email to receive OTP, user must click “Accept” to continue and an email with OTP will be send to user’s email address.</p> <p><i>-It is suggested for user to enable mobile OTP for optimal account security</i></p>	 
14	<p>User to input the OTP generated from mobile app or obtained from email and clicks “SUBMIT”</p>	
15	<p>User will be redirected to the homepage of DMS (for DA) / CCASS Terminal (for user)</p>	<p>For DA:</p> 

Change of Authentication Arrangement of CCASS Terminal Access Information Package for HKSCC CPs and DBs

#	Process	Sample Screenshot
		<p>For User:</p> 

Subsequent Login

#	Process	Sample Screenshot
1	DA access to DMS via https://www.ccass.com/dms / User access to CCASS Terminal via https://www.ccass.com/	<p>For DA:</p>  <p>For User:</p> 
2	During the parallel run, users can select the appropriate login method, user to click the appropriate button and proceed	

<p>3</p>	<p>User input the User ID and the password, and clicks “LOG IN”</p>	
<p>4</p>	<p>User to input the OTP generated from mobile app or obtained from email and clicks “SUBMIT”</p>	
<p>5</p>	<p>User will be redirected to the homepage of DMS (for DA) / CCASS Terminal (for user)</p>	<p>For DA:</p>  <p>For User:</p> 