

Change of Authentication Arrangement of CCMS Terminal Access

Information Package for HKCC and SEOCH Clearing Participants

Issue Date: December 2022

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	8
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	10
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	11
5.	Contact Information	11
6.	Checklist	12
Арр	endix A. Email registration procedure for users	13
Арр	endix B. 2FA Login Procedure	18

Modification History

Version	Date	Modified By	Synopsis
1.0	Oct 2022	HKCC & SEOCH	First draft
2.0	Dec 2022	HKCC & SEOCH	 Updated the following: 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.

1. Introduction

(Reference: As set out in the circular dated 1 September 2022 CD/OEC/HKCC/248/2022 and CD/OEC/SEOCH/249/2022) and 31 October 2022 (Reference: CD/OEC/HKCC/303/2022 and CD/OEC/SEOCH/304/2022), to enhance the security assurance, HKCC and SEOCH Clearing Participants (CPs) will progressively migrate to logging into CCMS 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 switching from smartcard to 2FA.

This Information Package aims to provide detailed information to assist CPs 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 will be notified via circular for information updates.

2. Overview of the Change of Authentication Method

2.1. Objective

In existing practice, a CCMS user must insert his/ her smartcard into the smartcard reader connecting to a CCMS Terminal and input a correct smartcard PIN to logon to CCMS Terminal. In order to enhance security assurance, HKEX is planning to replace the existing authentication method by 2FA, which means that users of CPs can logon to CCMS Terminal using a regular password together with an OTP generated by soft token via mobile application or email, instead of smartcard.

2.2. Migration from Smartcard to 2FA

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

For the preparation of using 2FA, CPs 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 CCMS 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 should follow the timeline to prepare for the implementation of 2FA accordingly. All CPs are encouraged to participate to access to CCMS 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 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 CCMS. In case users are not aware of their User ID, DAs can locate the User

ID of their users through CCMS Function – User Profile Listing, please refer to the detailed procedure listed in <u>Appendix A</u>. 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	HKCC CP	SEOCH CP
User ID for DAs	HK + Participant ID + 1/2/3/4 +	HK + Participant ID + X/Y/Z +
(to be assigned by HKEX)	X/Y/Z + 1-9, e.g. HKABC1X1	1/2/3/4 + 1-9, e.g. HKABC1X1
User ID for Users (existing users were assigned by HKEX, new users to be assigned by DAs upon the parallel run)	•	HK + Customer Code + 1/2/3/4 + 2 custom alphanumeric, e.g. HKABC101

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 <u>Google Playstore</u> for Android users and <u>Apple App Store</u> for iOS users. Users should refer to <u>Appendix B</u> 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:

	19 Dec 2022 Pre-parallel run	~Mid-Q2 2023 Commencement of parallel run	~Late-Q2 2023 End of parallel run
ų v	Login by smartcard only	Login by smartcard/ 2FA	Login by 2FA only
Кех	 Added new DMS user profile field: Email Create user profile for CPs & DBs Update DA's email address (available in early 2023) 	 DMS functions to be added: >DA to create & unlock user account 	 Remove existing DMS user profile fields: >SRN Applicable to >Certificate Expiry Date >martcard DMS function to be obsoleted >Reset Smartcard Password Remove user profile without email registration
DA	 Review the existing user list Input users' email address in DMS Maintain users profile in DMS 	Create & maintain users' profile in DMS	 Can assign DAs for business users group Maintain users' profile in DMS
L User		Setup password and login CCASS Terminal with 2FA	

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

	Pre-Parallel Run		Parallel Run		End of Par	End of Parallel Run	
User Maintenance	HKEX	DA	HKEX	DA	HKEX	DA	
DA User Profile							
Creation	\checkmark		\checkmark		\checkmark		
Profile	✓		✓		✓		
maintenance							
Email address	To be		To be		To be		
registration	announced		announced		announced		
Deletion	\checkmark		✓		✓		
Add business user					✓	\checkmark	
group functions							
User Profile							
Creation	\checkmark			\checkmark		\checkmark	
Profile		\checkmark		\checkmark		\checkmark	
Maintenance							
Email address		\checkmark		\checkmark		\checkmark	
registration							
Deletion		\checkmark		\checkmark		\checkmark	
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 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 CCMS 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	ENABLED						
Surname	TAIMAN						
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 CCMS 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 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 CCMS Terminal with 2FA following the procedure indicated in <u>Appendix B</u> 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 CCMS, except DAs can start to create users with reference to <u>Table 1</u>

The newly created users shall use 2FA as the authentication method to access CCMS 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 <u>Appendix B</u>. 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 CCMS 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 <u>Appendix B</u>.

3.2.3 Smartcard and smartcard reader maintenance

CPs could submit the maintenance request via eService SCard 1 – Smartcard Maintenance for User and DA in <u>Client Connect</u>, 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 CCMS Terminal via 2FA by then, and should continue to access by 2FA going forward. 2FA will be the sole authentication method to access CCMS Terminal since the time; smartcard authentication method will be obsoleted. 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, 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 CCMS and conduct settlement, should perform email update in DMS for the users of settlement agent.

4.2. User Creation

CP 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 <u>section 3</u>, 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. HKABC1X1 and HKABC101) 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 (HKABC1X1 and HKABC101) profile respectively

- 2. Commencement of Parallel Run:
 - Access CCMS Terminal for DA and users functions via the user ID HKABC1X1 and HKABC101 respectively by 2FA or smartcards, preferably 2FA
- 3. End of Parallel Run:
 - DA assigns business user groups to HKABC1X1 profile and DA removes the profile HKABC101
 - User holding HKABC1X1 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 CCMS Terminal. CPs 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 CCMS 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 CCMS user ID will be shown under "My Accounts", users should obtain OTP from such profile when accessing to CCMS Terminal. Meanwhile, CPs should note that users have to register separate soft token profiles and obtain OTP from respective profile to access CCMS Terminal.

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 <u>Client Connect</u> 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 CCMS Terminal access, please contact DCASS Hotline or Email indicated below:

- DCASS Hotline: +852 2979 7222 during normal office hours from 09:00 to 18:00 (Mondays to Fridays, excluding public holidays)
- DCASS Email: <u>ClearingPSD@hkex.com.hk</u>

6. Checklist

ITEM	IS TO BE CHECKED	\checkmark
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 CCMS 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

#	Process	Sample screenshot
1	Access to DMS via https://www.ccass.com/dms	← → C ↑ S https://www.ccass.com/dms
		HKEX 香港交易所
		HONG KONG EXCHANGES AND CLEARING LIMITED
		WELCOME TO CCASS/3
		SECURITY MANAGEMENT FUNCTIONS
		PLEASE INSERT YOUR SMARTCARD INTO THE READER BEFORE ENTERING PASSWORD. IF YOU ARE A FIRST TIME USER, PLEASE PRESS HERE UNITITALISE YOUR SMARTCARD.
		10 10 <td< td=""></td<>
2	Navigate to the View Listings tab and then click User Profile Listing ¹ tab from the menu bar	CASS/3 System - Internet Explorer File Edit View Favorites Tools Help HKEX 普捷交易所 User ID : B01254X1 Itanitatio User Profile Welcome Prof. Site Map. Logout. Charge Password. 19-Nov-22 16:07:56
		View Listings User Profile Listing View Listings User Profile Listing View Reports Disabled there Listing Disabled there Listing B01234X1 last access on 10-Nov-22 at 16:07:12
3	The profile of all their users including DA will be	
	displayed. DA can locate	Image: Second System Image: S
	the respective User ID	Norm :
	which is associated with the	DISAULDE AFTER : DISAULDE AFTER CCI CCI ACCESS CUMMER, :CT GI B BC MH I 11 12 11 15 11 15 11 14 1 CCI CM VERE STATUS : BNUMING W/ MH O DAT GP P 14 19 CP CP CP CP CP P1 P4 P5 F6 P7 PF P5 F6 PF P6 P6 F6 PF P1 P5 P5 F5 CP CP : CP :
	user name.	PS Q R1 R2 R3 R4 R5 R6 R7 R9 RA
		11.1 12 13 14 15 15 17 18 13 14, 15 12 13 14 15 15 17 18 13 14, 15 15 15 17 14 15 17 16 17 17 16 17 17 15 17 15 18 18 18 14 15 17 17 17 17 17 17 17 18 15 18 17 18 18 18 18 18
		AC 100 HZ 187 HO 184 HT 100 HV 184 KX BZ 5 45. 05 55 55 HT 55 KK 185 ST 57 T 0 V 18 X 121 H2 13 14 E1 50 T 1 0 V 18 X 121 H2 13 14 E1 50 T 10 V 18 X 121 H2 15 H2 15 H2 15 50 T 10 V 18 X 121 H2 15 H2 15 H2 15 50 T 12 H2 15 HT 100 T 12 H2 15 H2 15 50 T 12 H2 15 HT 100 T 12 H2 15 H2 15 50 T 12 H2 15 HT 100 T 12 H2 15 H2 15 50 T 12 H2 15 HT 100 T 12 H2 15 H2 15 50 T 12 H2 15 HT 100 T 12 H2 15 H2 15 50 T 12 H2 15 H2 15 H2 15 H2 15 H2 15 H2 15 50 T 12 H2 15 H2 15 H2 15 H2 15 H2 15 H2 15 50 T 12 H2 15 H2 15 H2 15 H2 15 H2 15 H2 15 H2 15 50 T 12 H2 15
		20 IR IS IT 20 IV IN IX II II BRIL:

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

¹ 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.

#	Process	Sample screenshot
1	Access to DMS via https://www.ccass.com/dms	← → C ↑ ③ https://www.ccass.com/dms
		音 港 交 易 所 HONG KONG EXCHANGES AND CLEARING LIMITED
		Image: Structure of the st
2	After locating the User ID, navigate to Maintain User Profile tab and then click Change User Profile ² tab from the menu bar	世 交 易 所 Maintain User Profile Delete U
3	Search user by entering "User ID" and click Submit	User ID :B01234X1 User ID :B01234X1 User Profile Print Site Map Logout Change Password 14-Dec-22 11:29:34 User ID Change User Profile - Prompt User ID User ID User Name Search by ④ User ID ⑥ User Name Search Filter *

For submitting request (to be performed by DA Maker)

² The Change User Profile function time in CCMS is 07:00 to 19:00 on Mondays to Fridays, and 09:00 to 13:00 on Saturdays, except for public holidays.



For authorizing request (to be performed by DA Checker)

#	Process	Sample se	creenshot				
1	On the same screen of submitting request performed by DA Maker, review and execute the request by entering "Checker ID" and "Authorization Code ³ ", then click Confirm	Haintain User Profile View Listings View Reports Reset Sourcland Don	User Profile Print Change User Profile - Confirm This is an end-user profile User ID User Status User ID User Status User ID User Status User ID User Status Cashing Control Translation Clearing House Options Transaction limits (HKD) Default IS Cash Compensation Indicator Cash Prepayment Selected User Groups 11 12 13 14 5 16 17 18 19 20 21 22 24 24 55 24 85 A AA AB AC AD CC OF OF PO PM Co RA AB DB DB UK AF AS AM ST WA WB WC WD WE WF WF Checker ID Authorisation Code	stion B0124601 ENABLED TAI MAN CHAN be@gabc.com.hk 01_Jan-03 Cash 9,999,999	1,090,099.39	DI Requirement Recall Request TI S Extended User Groups	5

³ DA Checker's Authorization Code can be obtained from the CCMS function - Get Authorisation Code. The Authorisation code will be renewed at the beginning of each month.

#	Process	Sample screenshot			
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.	Maintain User Profile Pist Sie Map Logout Change Password I View Liktings Change User Profile - Confirmation This is an end-user profile 00124001 User Status EXABLED User Status EXABLED User Status EXABLED User Status Change User Profile - Confirmation Train Label from 00124001 User Status EXABLED User Status EXABLED User Status EXABLED User Status Cash Transaction limit (HKD) 9,999,999,999,999,999,999,99 Disable after Cash Transaction limit (HKD) 9,999,999,999,999,999,99,99 Disable after Cash Transaction limit (HKD) 01 Require East Compensation Indicator A11 East Prepayment 5			
		SA SM ST WA WB WC WD WE WF WG THE ABOVE USER PROFILE IS CHANGED SUCCESSFULLY Modify Another User Profile	liste		

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	File Map Logout Change Password Lobeste User Profile Lobeste User Profile Logon Success View Reports
2	Enter the User ID and click Submit	Enquire User Profile Print Site Map Logout Change Password 14-Dec-22 13:58:04 I View Listings I View Reports
		User ID Submit
		Search by User ID User Name
		Search Filter *
		List Refresh Help

#	Process	Sample screenshot	
3	The detailed user profile will	CLASS/3 System - Internet Supioner - File Edit. View Favorites Tools Help Deer nu - W	
	be displayed		UPE 03
		This is an ond user profile SRI (for user grantance) Gentificate Carity Date Gentificate Carity	E EI 15 P6 RL 12 Y3
4	For DAs who want to	ZW ZX ZY ZZ Enquire Another User Profile Back.	×
	download the latest user profile listing, can navigate to the View Listings tab and then click User Profile Listing ⁴ tab from the menu	File Edit View Favorites Tools Help 日本になります。 普捷交易所 User ID : B01234X1 Haintain User Profile Waldcome Print Ste Map Logout Change Password 10-Nov-22 1607:56 View Listing User Profile Listing User Profile Listing	
	bar	1 View Reports Deskide View Latterg 1 Reset Smartcard Pred ISBN Listing 1 Reset Smartcard Pred B01234X1 Tast access on 10-Nov-22 at 16:07:12	
5	The User Profile Listing with User ID, registered email address and the user account details will be generated		□ × ∩ ☆ ⑬ •• •• •* ,999-00

⁴ 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 CCMS Terminal via https://www.ccass.com/	For DA: $\leftrightarrow \rightarrow \mathbb{C} \ \bigtriangleup \ \texttt{https://www.ccass.com/dms}$ For User: $\leftarrow \rightarrow \mathbb{C} \ \bigtriangleup \ \texttt{https://www.ccass.com/}$
2	During the parallel run, users can select the appropriate login method, user to click the appropriate button and proceed	推 送 交 現 所 Login with OTP Login with Smart card
3	Users to click "Forgot/Reset your Password" button on the login page	ドレンション Set A
4	A pop-up window will be displayed, user input their User ID and clicks "SUBMIT" button	ドレビディン Provide Address Provided Addre

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	CCASS : One Time Password From noreply_pt@hkex.com.hk L* Date Today 17:30 One Time Password (OTP) for CCASS: 27788148 Please Enter Your One Time Password, Or Request A New One SUBMIT OTP REQUEST OTP
6	User input new password twice to complete the setup of their password	Eree Password Reset Password Reset reset your password below. Luable to reset your password New password has been used previously. Password Confirm password LUBMIT Close
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	一日 一日 一日 一日 一日 一日 一日 一日 一日 一

8	User input the User ID and the newly set password, and clicks "LOG IN"	HKEに 重 准 交 面 府 Welcome to CCASS User Login User ID Personal Per
9	The system will ask user to register the mobile devices for the 2FA. User clicks "REGISTER DEVICE"	нкех ##Х## Welcome to CCASS
10	User to search "ForgeRock Authenticator" from Google Play or Apple's App Store	ForgeRock Authenticator Image: Constraint of the second secon
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.	HKEX Welcome to CCASS Image: CMHK Image: Left 11:01 Physical Components Edit
12	User to click the account from mobile app and then click C to generate a OTP	ForgeRock B0123401 All CMHK ♥ L4♥ 11:01 CH My Accounts ForgeRock B0123401 One-time Password Ø 814 929 CH

13	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. -It is suggested for user to enable mobile OTP for optimal account security	<section-header></section-header>
14	User to input the OTP generated from mobile app or obtained from email and clicks "SUBMIT"	HKEX 意識文目前 Welcome to CCASS Enter verification code SUBMIT
15	User will be redirected to the homepage of DMS (for DA) / CCMS Terminal (for user)	For DA: 香港交易所 User ID : B01246X1 Logont Change Password 04-Dec-22 11:28:34 User ID : B01246X1 User ID : B0

	For User:				
	General Enquiries Enq Settlement Act / Status Delivery Instruction (DI) A/C Transfer Instr (ATI)	Maintain Broadcast Message	Site Map Announcement Information	Last access on 30-Apr-82 at 15:44:46 Broadcast Message Report Download Change Print Logout Password	B0350401 MMBE 01 30-Apr-02 15:47
	Settlement Instruction (SI) Investor Stm Instr (ISI)	Enquire Broadcast Messag Market Code			
	ISI Counterparty List Payment Instruction Cash Prepayment	Market Code Broadcast Message Type		rmative C Event Completion C Emerger	ъсу
	Stock Borrowing / Lending SBL Bulletin Board General Stock Collateral		List	Refresh	Help
	Login Withdrawal Order Election Instruction				
	Subscription Instruction Corp Voting Instruction EIPO Application				
	Tender Instruction Corp Communication				
	Upload Batch File Report Profile Maintenance View Circular				
	Start: applet not initialized.			🕒 🥑 Internet	

Subsequent Login

#	Process	Sample Screenshot
1	DA access to DMS via https://www.ccass.com/dms / User access to CCMS Terminal via https://www.ccass.com/	For DA: $\leftarrow \rightarrow \mathbb{C} \ \bigtriangleup \ https://www.ccass.com/dms$ For User: $\leftarrow \rightarrow \mathbb{C} \ \bigtriangleup \ https://www.ccass.com/$
2	During the parallel run, users can select the appropriate login method, user to click the appropriate button and proceed	推交 熟 所 Login with OTP Login with Smart card

3	User input the User ID and the password, and clicks "LOG IN"	使意で変更新 Welcome to CCASS Input User ID User ID SUBMIT
4	User to input the OTP generated from mobile app or obtained from email and clicks "SUBMIT"	ビアン ドアン ドアン ドアン ドアン ドアン ドアン ドアン ドアン ドアン ド
5	User will be redirected to the homepage of DMS (for DA) / CCMS Terminal (for user)	For D.E. Image: Start Sta