



Change of Authentication Arrangement for Terminal Access to CCASS/ CCMS

— Launch of Two-Factor Authentication Preparation Briefing

Operations Division

24, 25 and 26 April 2023

Agenda

- 01 | Background
- 02 | 2FA Operations
- 03 | Implementation Approach of 2FA
- 04 | Important Information
- 05 | What's Next?
- 06 | Enquiries and Support
- 07 | Checklist
- 08 | Appendices



1. Background

- Overview

To enhance security assurance, Two-Factor Authentication (2FA) is introduced to replace the existing smartcard and smartcard reader authentication.

		By Smartcard (TODAY)	By 2FA (Mid-2023 Tentatively)
User ID		<ul style="list-style-type: none"> 8 character code 	8 character code <i>(same as existing)</i>
Authentication Method		<ul style="list-style-type: none"> Smartcard & smartcard reader Smartcard PIN 	<ul style="list-style-type: none"> Regular password NEW OTP obtained from mobile application / email
User Maintenance	CCASS/ CCMS Delegated Administrator (DA)	<ul style="list-style-type: none"> User profile maintenance by HKEX 	<ul style="list-style-type: none"> User profile maintenance by HKEX Can be assigned with business users group function <i>(to be available in later stage)</i> NEW
	CCASS/ CCMS User (User)	<ul style="list-style-type: none"> User profile maintenance by DA <i>(except account creation by HKEX)</i> 	<ul style="list-style-type: none"> User profile maintenance by DA User account creation by DA NEW

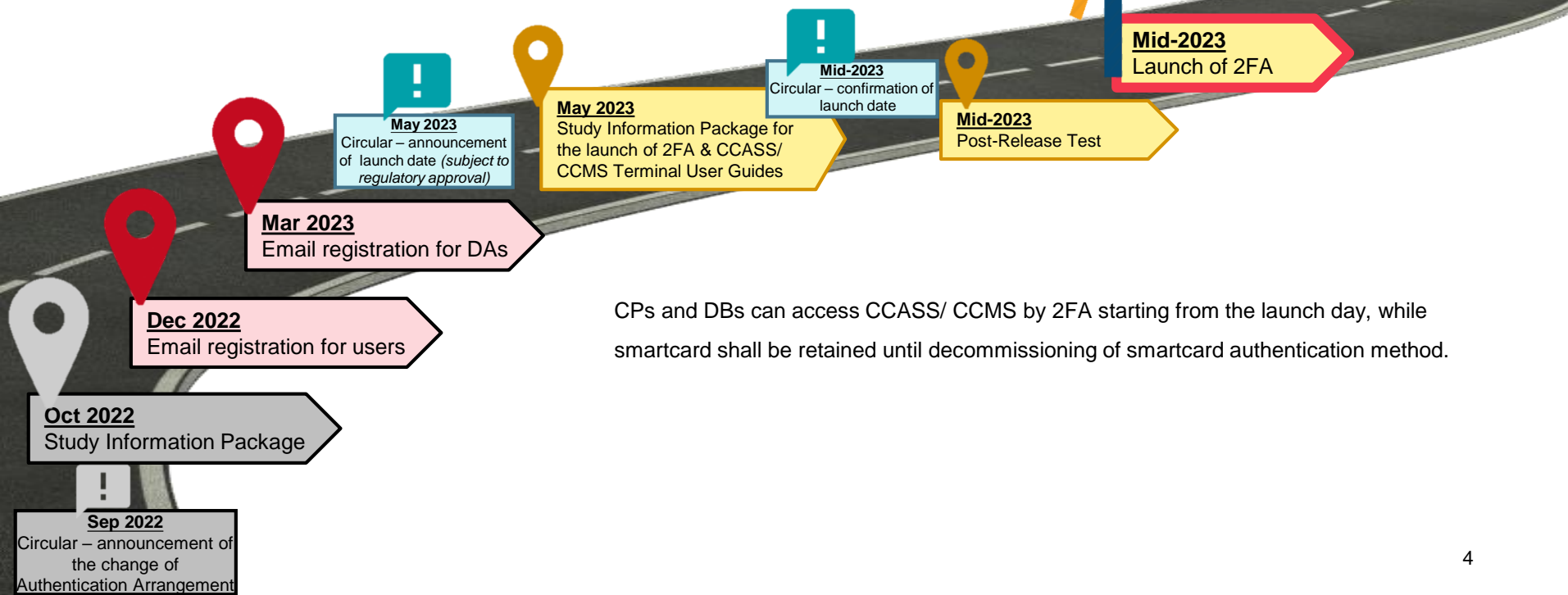
HKSCC CPs and DBs who access to CCASS through Participant Gateway (PG) will not be impacted, and should remain accessing to CCASS via smartcard.

The changes will only be applied on the authentication method of Terminal access to CCASS/ CCMS, including Security Management Functions (DMS) and Overnight Report Distribution (ONRD) function, while the terminal functions and operations remain unchanged.

1. Background (Cont'd)

- Timeline

HKEX has arranged the following activities to ensure a smooth transition for Participants of HKSCC, HKCC and SEOCH (CPs) and HKSCC Designated Banks (DBs) for migrating to logging into CCASS/ CCMS by 2FA:




CPs and DBs can access CCASS/ CCMS by 2FA starting from the launch day, while smartcard shall be retained until decommissioning of smartcard authentication method.

2FA Operations



2. 2FA Operations - DAs

- 1 Authentication
- 2 DA Creation
- 3 DA Maintenance

Today	VS	Launch of 2FA
<ul style="list-style-type: none">• Smartcard	<div>NEW</div> <ul style="list-style-type: none">• 2FA• Smartcard (reserved) <i>DAs created upon launch of 2FA can only access by 2FA.</i>	
<ul style="list-style-type: none">• By HKEX (submit eService SCard 1)	<div>NEW</div> <ul style="list-style-type: none">• By HKEX (submit eService DA 3 - <i>refer to the assigned User ID in DA 3 that is being processed by HKEX</i>)	
<ul style="list-style-type: none">• By HKEX (submit eService SCard 1)	<div>NEW</div> <ul style="list-style-type: none">By HKEX (submit eService DA 3) <div> DAs can be assigned with business user role upon the decommissioning of smartcard</div>	

eService DA 3

MAINTENANCE REQUEST

Maintenance Request

Multiple selection is allowed

☒ Add

☐ Change





☐ Unlock/ Enable/ Disable

☐ Delete

To be enriched with more maintenance request types upon the launch of 2FA

2. 2FA Operations (Cont'd)

- DAs

		Today	VS	Launch of 2FA
4	Password Reset			
a	Enabled mobile app OTP	<ul style="list-style-type: none">N/A		Self-served password reset by Forgot/ Reset Password function
b	Enabled email OTP	<ul style="list-style-type: none">N/A		By HKEX (Submit eService DA 3)
c	<u>Forgot smartcard password</u>	<ul style="list-style-type: none">By HKEX (Submit eService SCard 1)		
5	Account Unlock	<ul style="list-style-type: none">N/A		By HKEX (Submit eService DA 3)

eService SCard 1 will only be available for Smartcard Password Reset upon the launch of 2FA, CPs and DBs should submit eService DA 3 for any other DA maintenance by then.



For details of the procedure, please refer to Appendix 1.






2. 2FA Operations (Cont'd)

- Users

	Today	VS	Launch of 2FA
1 Authentication	<ul style="list-style-type: none">Smartcard	<div>NEW</div> <ul style="list-style-type: none">2FA<ul style="list-style-type: none">Smartcard (reserved) <i>Users created upon launch of 2FA can only access by 2FA.</i>	
2 User Creation	<ul style="list-style-type: none">By HKEX	<div>NEW</div> <ul style="list-style-type: none">By DA (Assumption: available user accounts)	
3 User Maintenance	<ul style="list-style-type: none">By DA		

2. 2FA Operations (Cont'd)

- Users

		Today	VS	Launch of 2FA
4	Password Reset			
a	Enabled mobile app OTP	<ul style="list-style-type: none">N/A		<ul style="list-style-type: none">Self-served password reset by Forgot/ Reset Password function
b	Enabled email OTP	<ul style="list-style-type: none">N/A		<ul style="list-style-type: none">Unlock/ Reset OTP Device Registration by DA
c	<u>Forgot smartcard password</u>	<ul style="list-style-type: none">Smartcard Password Reset by DA		
5	Account Unlock	<ul style="list-style-type: none">N/A		<ul style="list-style-type: none">Reset account by DA

For details of the procedure, please refer to Appendix 1.



2. 2FA Operations (Cont'd)

- Users Migration

Today

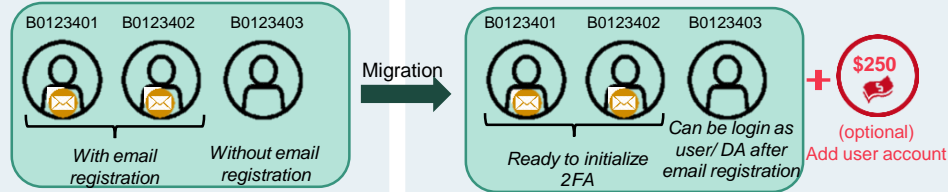
VS

Launch of 2FA

1

User account migration

All the existing user accounts with smartcards (with or without email registration) will be migrated to 2FA, CPs & DBs can refer to **User Profile Listing** for the existing user profile:
An example of the user account migration is illustrated below:



2

Apply new user account

For users and DAs:

- Submit eService SCard 1 for DA and user maintenance & SCard 3 for ordering smartcard reader
- one-off fee: \$300/ smartcard reader & \$250/ smartcard

For users and DAs:

- Submit eService **DA4**
- one-off fee: **\$250/ user account**
- **Smartcard and smartcard reader are no longer available for purchase.**

DA's can access to User Profile Listing function in DMS to check the total number of users available after.

MAX NO. OF USERS	: 20
TOTAL NO. OF USERS	: 16
TOTAL NO. OF DELEGATED ADMINISTRATORS	: 6
TOTAL NO. OF USERS EXCEPT DELEGATED ADMINISTRATORS	: 10



2. 2FA Operations (Cont'd)

- Users Migration

Today

VS

Launch of 2FA

3

DA's Right

User Maintenance

4

DMS Functions

- (Since Dec 2022)
Added "Email" field - to register email for their users

Email



- DA can create user profile and assign User ID for their users

Create User Profile - Detail	
This is an end-user profile	
Organisation	B01234 ABC SECURITIES
Internal/External	EXTERNAL
User ID	B01234 Generate User ID
User Status	<input checked="" type="radio"/> ENABLED <input type="radio"/> DISABLED
Surname	
Other Names	
Email	
Enable From	<input type="text"/> DD/MM/YY
Disable After	<input type="text"/> DD/MM/YY
Clearing House Options	Cash
Access Channel	CST



- DA can assign business user group(s) to users upon the decommissioning of smartcard



- Upon 2FA initialization:

The following fields will be available in the user profile:

Locked	No <input type="radio"/> Unlock/Reset OTP Device Registration
OTP Enabled	Yes

While the following fields will be remove:

SRN (for user using smartcard)	0101101200012AB2
Certificate Expiry Date	31-Dec-30 23:59:59

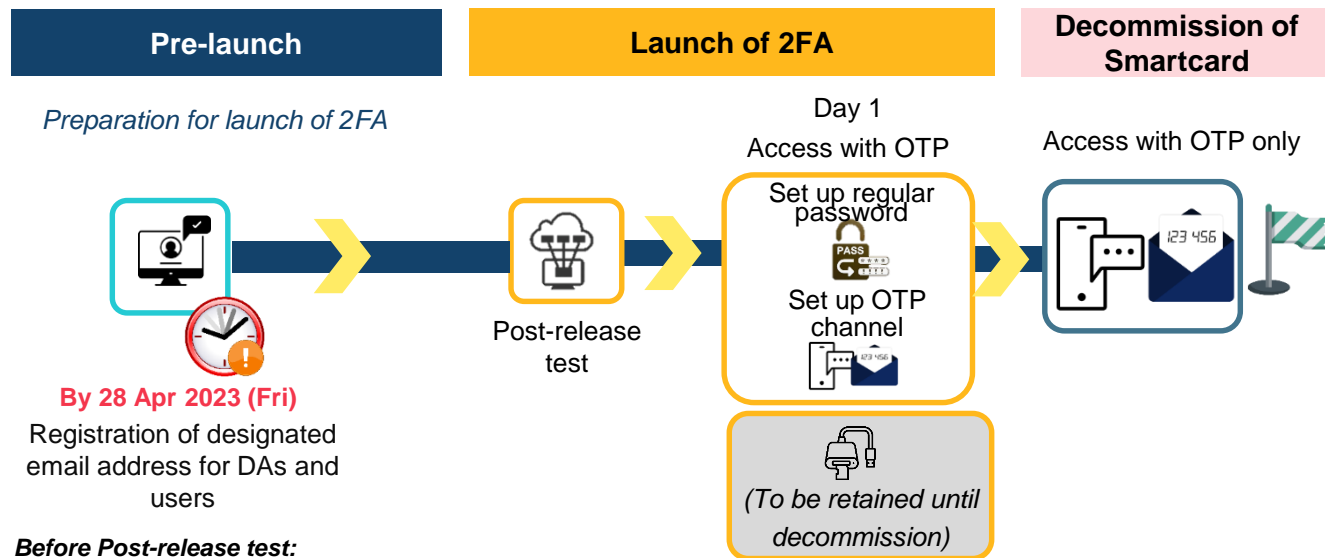
Vice versa for user who have yet to initialize 2FA.
(can only view under "Enquiry User Profile" and "Delete User Profile" functions).

3. Implementation Approach of 2FA



3. Implementation Approach of 2FA

The following is a high level implementation approach for transition from smartcard to 2FA:



Before Post-release test:

- ✓ Complete the email registration
(Refer to Appendix 2 for details)
- ✓ Perform connectivity verification
- ✓ Check CCASS / CCMS Terminal URL bookmarks
<https://www.ccass.com>

3. Implementation Approach of 2FA (Cont'd)



Upon the launch of 2FA, users and DAs should initialize 2FA immediately.



User ID remains unchanged

	HKSCC CPs	HKSCC DBs	HKCC CPs	SEOCH CPs
User ID for DAs (to be assigned by HKEX)	Participant ID + X/Y/Z + 1-9, e.g. B01234X1	Participant ID + X/Y/Z + 1-9, e.g. BNK999X1	HK + Participant ID + 1/2/3/4 + X/Y/Z + 1-9, e.g. HKABC1X1	HK + Participant ID + X/Y/Z + 1/2/3/4 + 1-9, e.g. HKABC2X1
User ID for Users (existing users were assigned by HKEX, new users to be assigned by DAs upon the launch of 2FA)	Participant ID + 2 custom alphanumeric, e.g. B0123401	Participant ID + 2 custom alphanumeric, e.g. BNK99901	HK + Customer Code + 1/2/3/4 + 2 custom alphanumeric, e.g. HKABC101	HK + Customer Code + 1/2/3/4 + 2 custom alphanumeric, e.g. HKABC201



Modified

To be elaborated in the later slides

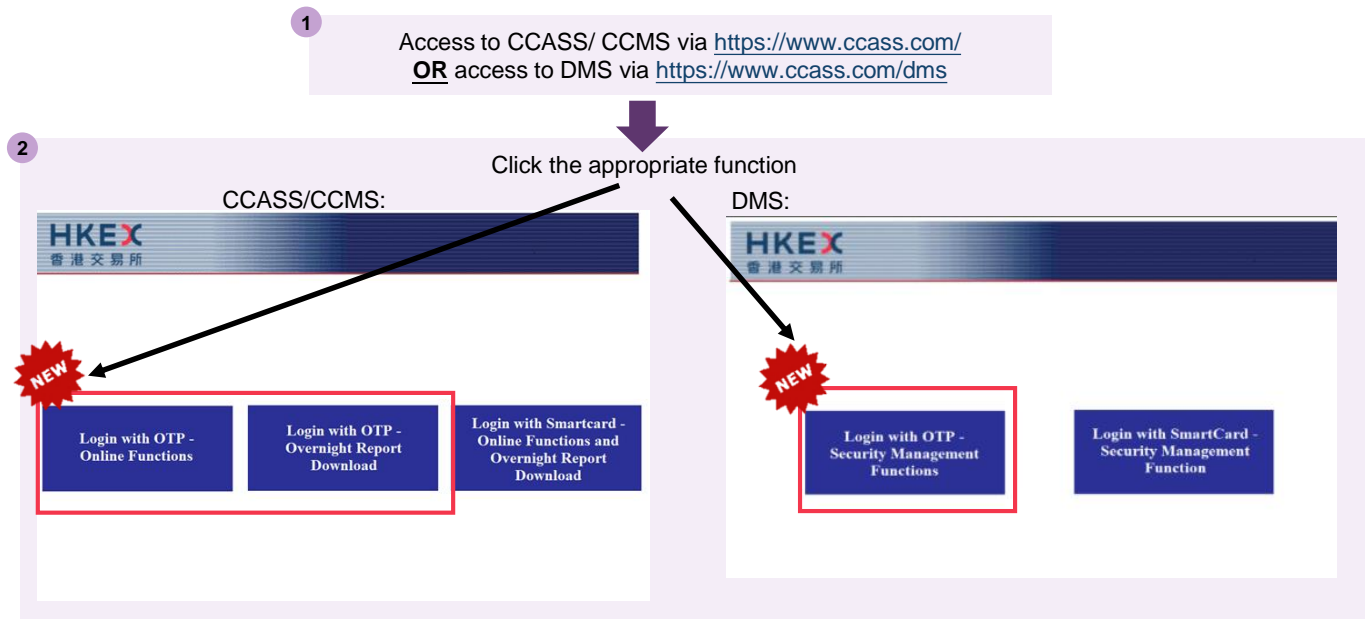
Step by step procedure to be shared in the following slides



3. Implementation Approach of 2FA (Cont'd)



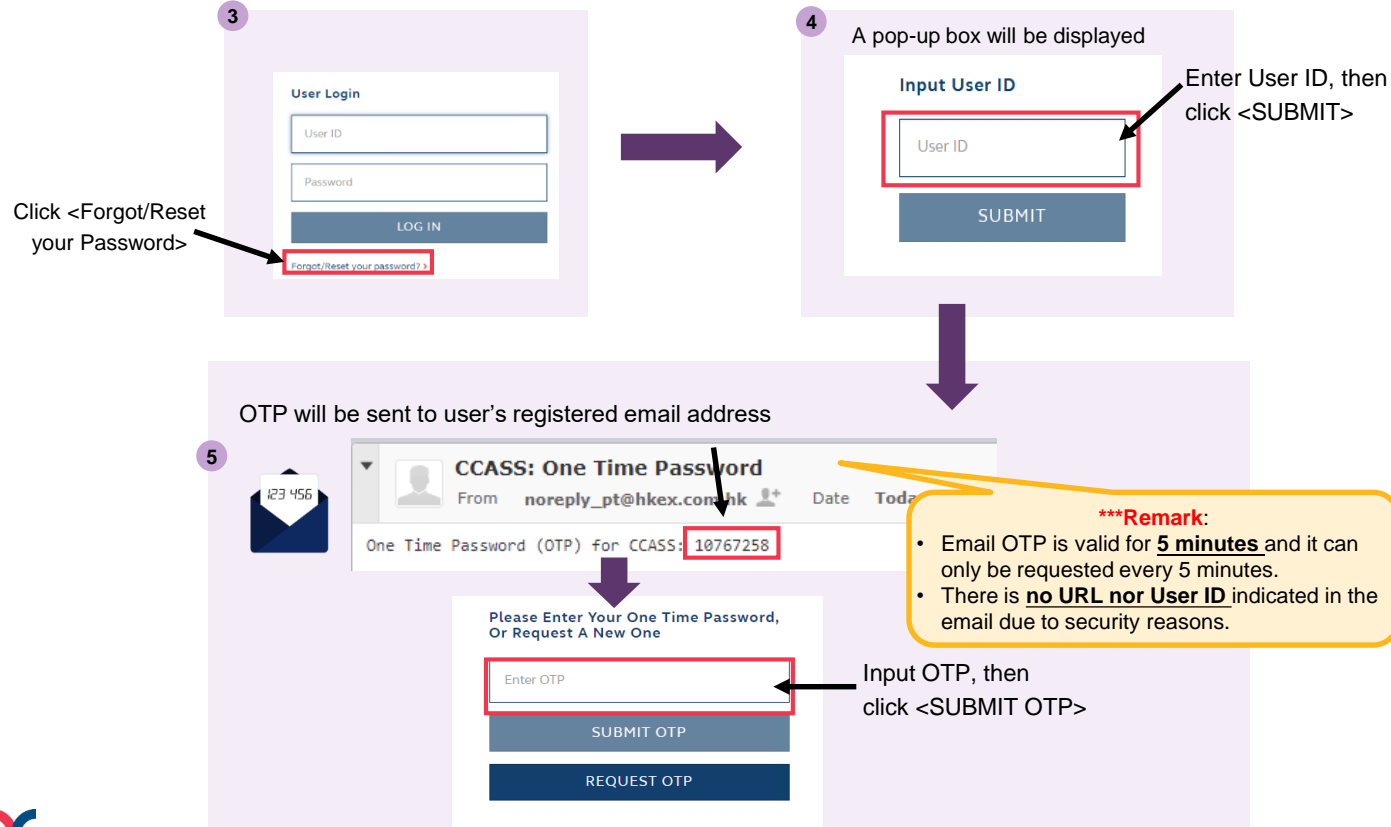
1. Set up password:



3. Implementation Approach of 2FA (Cont'd)



1. Set up password (cont'd):



3. Implementation Approach of 2FA (Cont'd)

1. Set up password (cont'd):



6

Input new password twice, then click <SUBMIT>

HKEX
香港交易所

Reset Password

Please enter your new password below.

Password

Confirm password

SUBMIT

Close

Set up the password based on password requirements:

1. At least 16 characters
2. At least 1 number
3. At least 1 lower letter
4. At least 1 special character from !@#%&*()
5. At least 1 capital letter

7

Password changed successfully, click <Close>

HKEX
香港交易所

Reset Password

Your password has been successfully reset.

Close

The pop-up box will be closed

3. Implementation Approach of 2FA (Cont'd)

2. Set up OTP Channel:



8 Return to the login page

CCASS/CCMS:

HKEX
香港交易所

WELCOME TO CCASS

User Login

User ID

Password

LOG IN

[Forgot/Reset your password? >](#)

By clicking the 'LOG IN' button, I confirm that the individual(s) whose personal data is disclosed in my use of this application consent to the processing of their personal data.

Unauthorised access and use are prohibited, HKEX reserves the right to take actions against offenders.

Enter User ID and Password, then click <LOG IN>

DMS:

HKEX
香港交易所

WELCOME TO CCASS SECURITY MANAGEMENT FUNCTIONS

User Login

User ID

Password

LOG IN

[Forgot/Reset your password? >](#)

By clicking the 'LOG IN' button, I confirm that the individual(s) whose personal data is disclosed in my use of this application consent to the processing of their personal data.

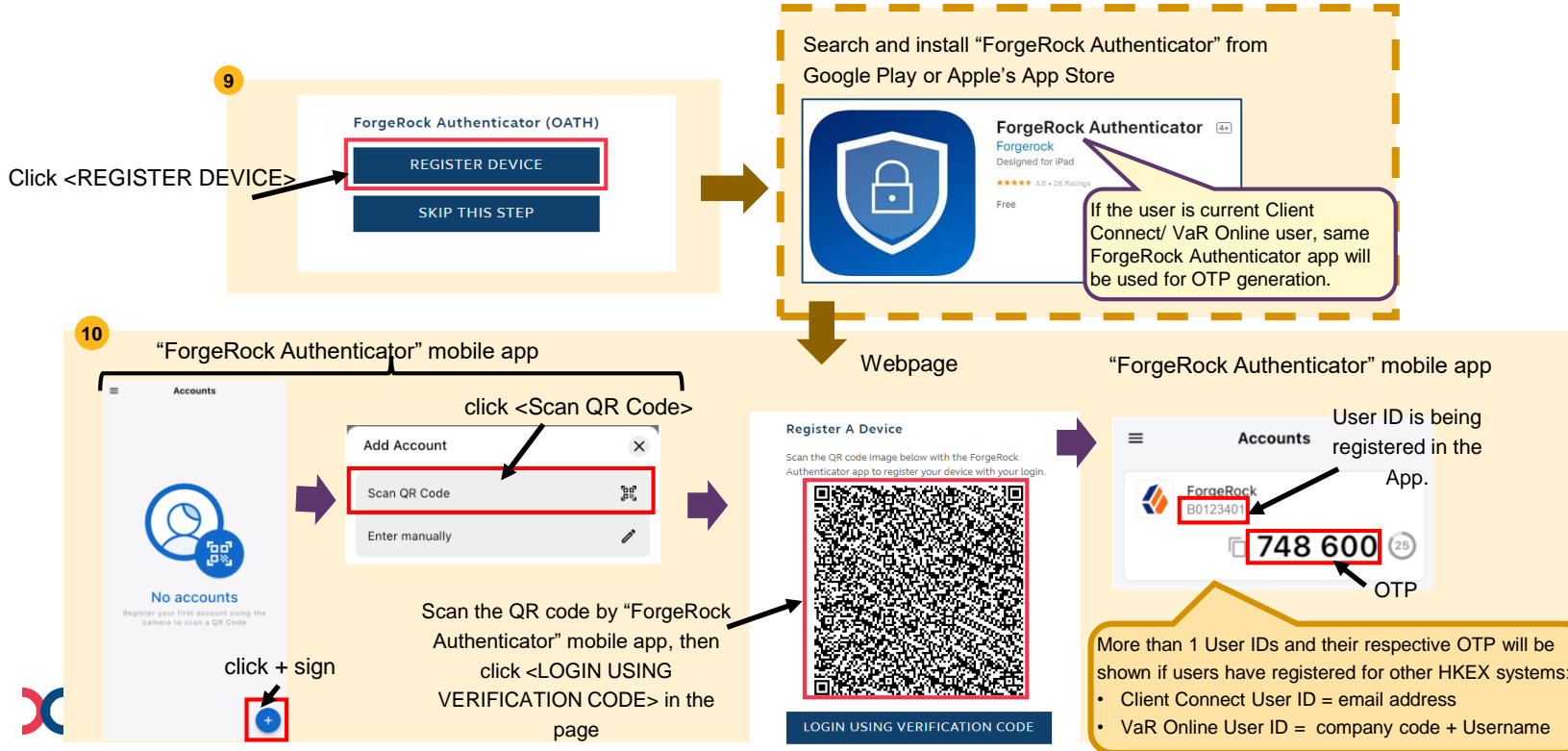
Unauthorised access and use are prohibited, HKEX reserves the right to take actions against offenders.

3. Implementation Approach of 2FA (Cont'd)



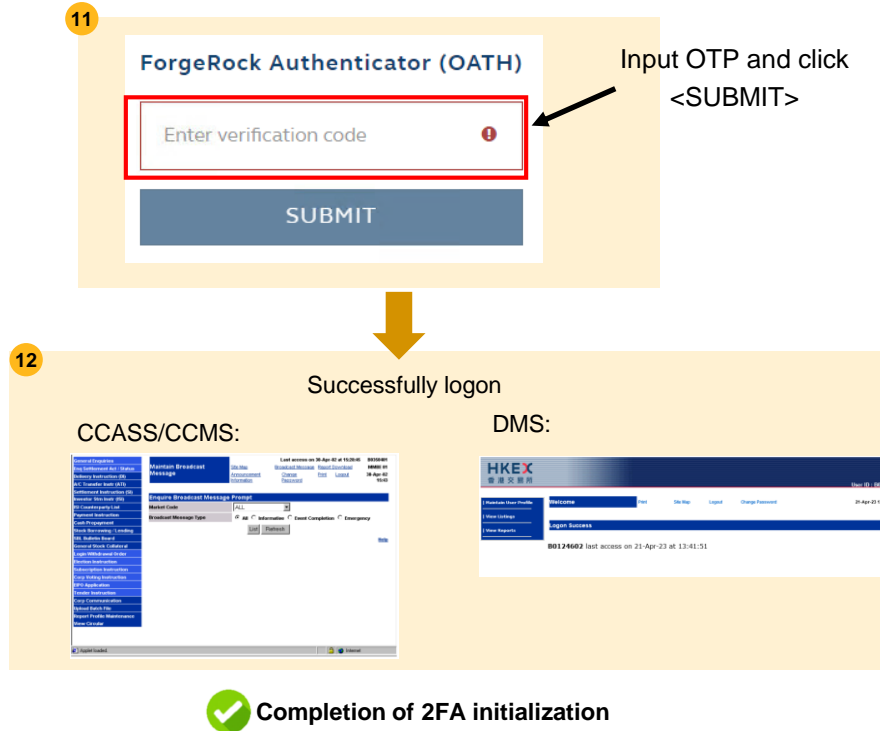
2a. Set up OTP Channel (Mobile App):

 **For users who prefer to receive OTP via mobile App**
suggested for optimal account security and maintenance function 



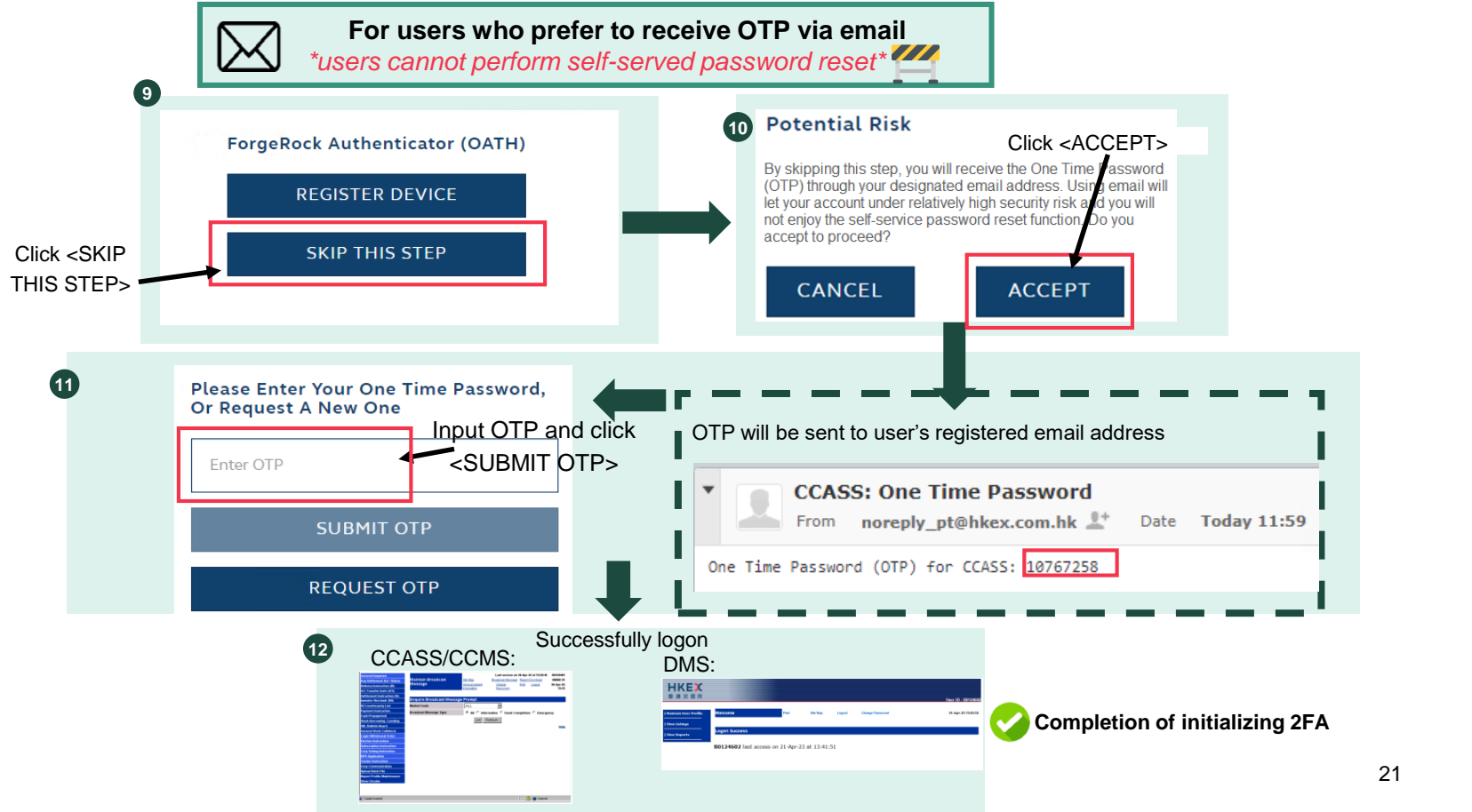
3. Implementation Approach of 2FA (Cont'd)

2a. Set up OTP Channel (Mobile App):



3. Implementation Approach of 2FA (Cont'd)

2b. Set up OTP Channel (Email):



3. Implementation Approach of 2FA (Cont'd)

3. On-going login with 2FA:



Access with OTP

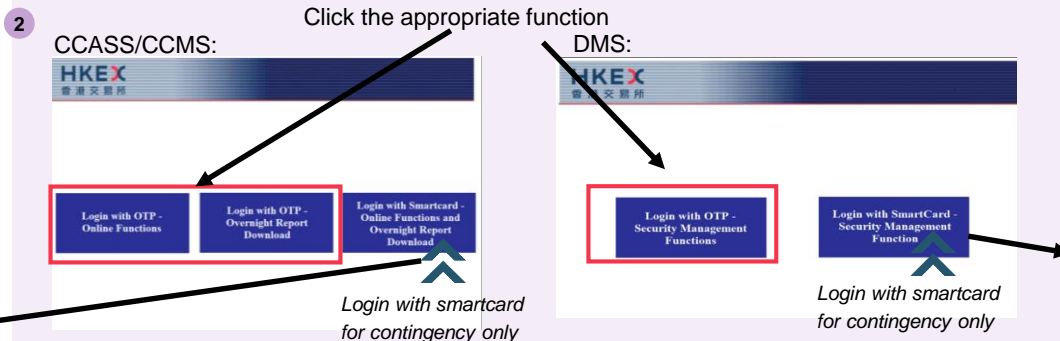


If user clicks <Login with Smartcard>, it will be redirected to the current CCASS/ CCMS login page.



Then login by the existing flow

1 Access to CCASS/ CCMS via <https://www.ccass.com/>
OR access to DMS via <https://www.ccass.com/dms>



If DA clicks <Login with Smartcard>, it will be redirected to the current DMS login page.



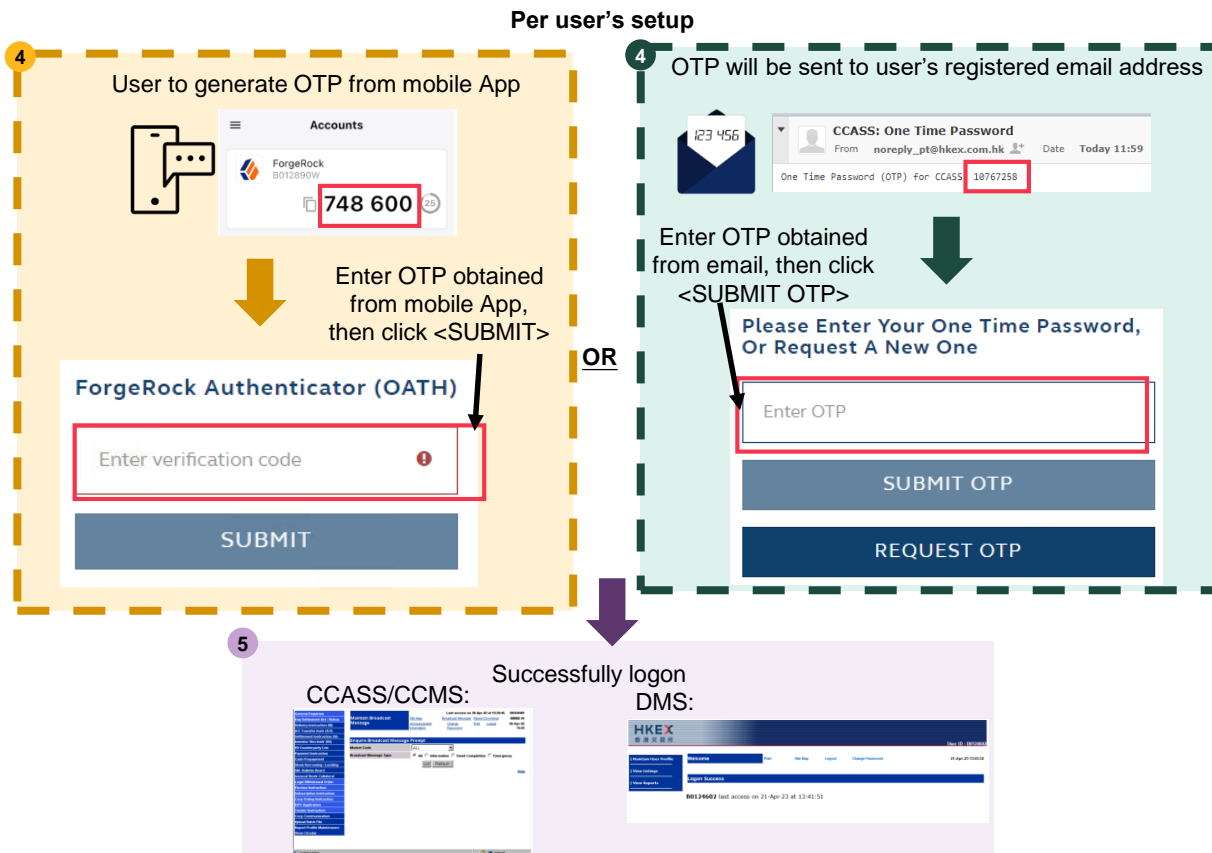
Then login by the existing flow



3. Implementation Approach of 2FA (Cont'd)



3. On-going login with 2FA (Cont'd):



3. Implementation Approach of 2FA (Cont'd)

After smartcard decommissioned



Access with OTP



Smartcard authentication is decommissioned

1

Access to CCASS/ CCMS via <https://www.ccass.com/>
OR access to DMS via <https://www.ccass.com/dms>

2

Select the appropriate function

CCASS/CCMS:

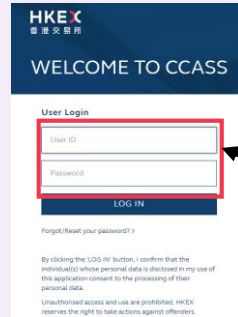


3



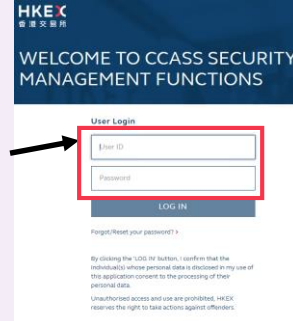
3

CCASS/CCMS:



Enter User ID and Password, then click <LOG IN>

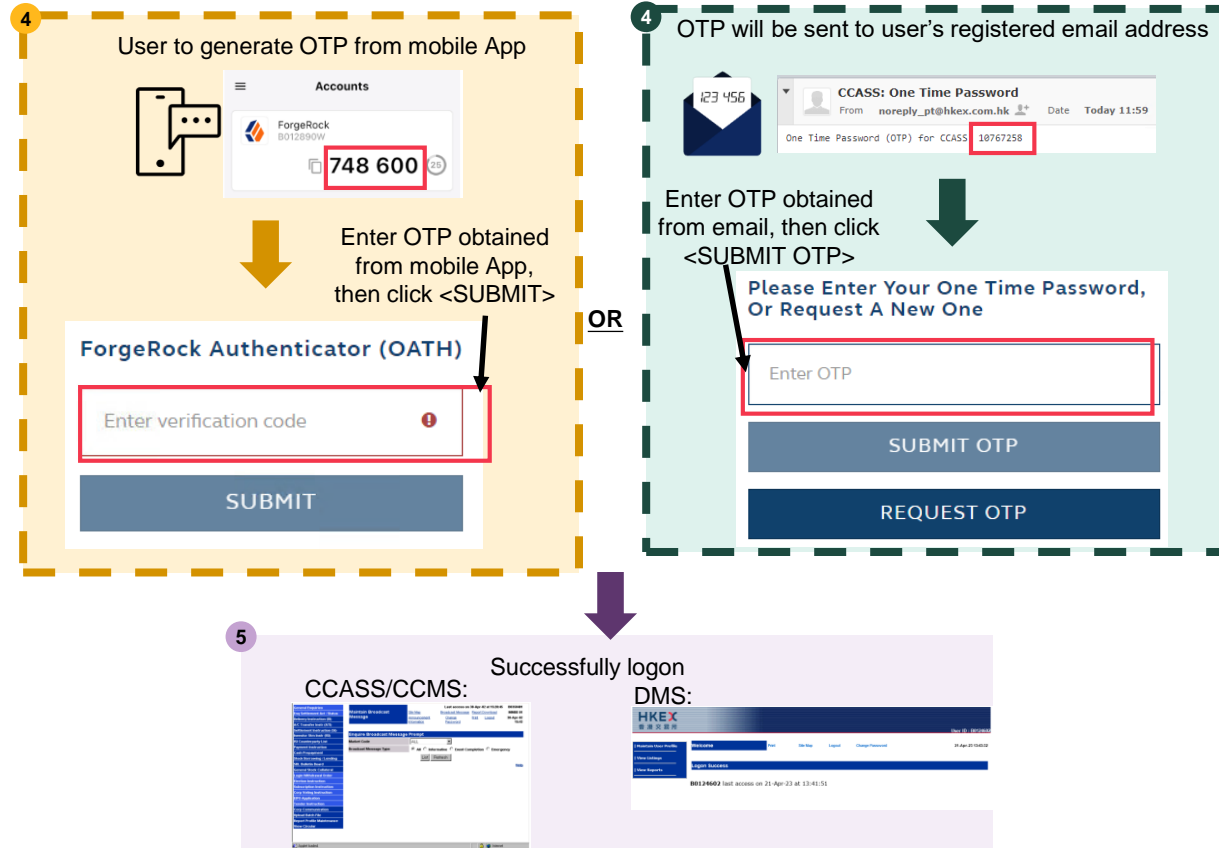
DMS:



3. Implementation Approach of 2FA (Cont'd)



Per user's setup



Important Information



4. Important Information

1. Retaining your Smartcard and Smartcard reader

If you are PG users, you should retain your smartcard and smartcard reader. CPs and DBs should not dispose their smartcards and smartcard readers until the decommissioning of smartcard.

2. Backup Centre

Upon the launch of 2FA, CPs and DBs can only use 2FA to login CCASS/ CCMS at Backup Centre.



What's Next?



5. What's Next?

- More Information regarding the change of authentication method are available on HKEX website, please visit the website regularly for the latest information.

For HKSCC CPs & DBs

CHANGE OF AUTHENTICATION ARRANGEMENT OF CCASS TERMINAL ACCESS

To enhance security assurance, CCASS Participants (CPs) and Designated Banks (DBs) will progressively migrate to logging into CCASS from smartcard to Two-Factor Authentication (2FA). To ensure a smooth transition for CPs and DBs switching from smartcard to 2FA, a parallel run for both authentication methods will be provided. The following materials are to facilitate CPs and DBs to prepare for the parallel-run:

Guideline and Information Package

- Guideline for Email Registration for CCASS/ CCMS Delegated Administrators (Feb 2023)
- Information Package for HKSCC Participants and Designated Banks (Dec 2022)

Circulars

- Change of Authentication for CCASS Terminal – (i) Reminder of Email Registration for CCASS Users and Delegated Administrators; (ii) Briefings for the Launch of Two-Factor Authentication Preparation (Apr 2023)
- Change of Authentication for CCASS Terminal – (i) Reminder of email registration for CCASS users; (ii) Kick-off of email registration for CCASS Delegated Administrators (Feb 2023)
- Change of Authentication for CCASS Terminal – Kicking off Email Registration (Dec 2022)
- Information Package for the Change of Authentication for CCASS Terminal Access (Oct 2022)
- Change of Authentication Arrangement of CCASS Terminal Access (Sep 2022)

For Clearing Participants, please visit [webpage](#).

For HKCC & SEOCH CPs

CHANGE OF AUTHENTICATION ARRANGEMENT OF CCMS TERMINAL ACCESS

To enhance security assurance, Clearing Participants (CPs) will progressively migrate to logging into CCMS from smartcard to Two-Factor Authentication (2FA). To ensure a smooth transition for CPs switching from smartcard to 2FA, a parallel run for both authentication methods will be provided. The following materials are to facilitate CPs to prepare for the parallel-run:

Guideline and Information Package

- Guideline for Email Registration for CCASS/ CCMS Delegated Administrators (Feb 2023)
- Information Package for HKCC and SEOCH Clearing Participants (Dec 2022)

Circulars

-For HKCC:

- Change of Authentication for CCMS Terminal – (i) Reminder of Email Registration for CCMS Users and Delegated Administrators; (ii) Briefings for the Launch of Two-Factor Authentication Preparation (Apr 2023)
- Change of Authentication for CCMS Terminal – (i) Reminder of email registration for CCMS users; (ii) Kick-off of email registration for CCMS Delegated Administrators (Feb 2023)
- Change of Authentication for CCMS Terminal – Kicking off Email Registration (Dec 2022)
- Information Package for the Change of Authentication for CCMS Terminal Access (Oct 2022)
- Change of Authentication Arrangement of CCMS Terminal Access (Sep 2022)

-For SEOCH:

- Change of Authentication for CCMS Terminal – (i) Reminder of Email Registration for CCMS Users and Delegated Administrators; (ii) Briefings for the Launch of Two-Factor Authentication Preparation (Apr 2023)
- Change of Authentication for CCMS Terminal – (i) Reminder of email registration for CCMS users; (ii) Kick-off of email registration for CCMS Delegated Administrators (Feb 2023)
- Change of Authentication for CCMS Terminal – Kicking off Email Registration (Dec 2022)
- Information Package for the Change of Authentication for CCMS Terminal Access (Oct 2022)
- Change of Authentication Arrangement of CCMS Terminal Access (Sep 2022)

For CCASS Participants and Designated Banks, please visit [webpage](#).



- Information Package for the launch of 2FA and the updated Terminal User Guide will be available in HKEX website in May 2023.



Enquiries and Support



6. Enquiries and Support

For any enquiries about the change of authentication arrangement of Terminal access to CCASS/ CCMS, please contact CCASS/ DCASS Hotline or Email indicated below:



Terminal	CCASS	CCMS
	2979 7111	2979 7222
Hotline	<i>During normal office hours from 09:00 to 18:00 (Mondays to Fridays, excluding public holidays)</i>	
Email	ClearingPS@hkex.com.hk	ClearingPSD@hkex.com.hk

Checklist



7. Checklist



Checklist for CPs and DBs to prepare for the launch of 2FA:		<input checked="" type="checkbox"/>
1	Register the designated email for all users and DAs for the regular password setup	<input type="checkbox"/>
2	Check CCASS/ CCMS Terminal bookmarked URL	<input type="checkbox"/>
3	Perform connectivity verification for new CCASS/ CCMS 2FA servers <i>-Reference to circulars dated 3 April 2023 (HKSCC: CD/OES/CCASS/013/2023, HKCC: CD/OEC/HKCC/092/2023 and SEOCH: CD/OEC/SEOCH/093/2023)</i>	<input type="checkbox"/>
4	Inform all users and DAs in your company for the change of authentication arrangement	<input type="checkbox"/>
5	Study the Information Package for Launch of 2FA and the updated CCASS/ CCMS terminal user guides (available in May 2023)	<input type="checkbox"/>
6	Understand the first time login procedure for 2FA	<input type="checkbox"/>
7	If the user is current Client Connect/ VaR Online user, same ForgeRock Authenticator app will be used for OTP generation.	<input type="checkbox"/>

Q & A Session



Appendices



8. Appendix 1 – Account Maintenance for Users and DAs

The following table has summarized the type of account maintenance and the corresponding action required under 2FA:

Type of Account Maintenance

Action Required

1 Password Change

a

Self-served by Change Password function

- Password should be changed at least every 90 days. Once the password is expired, user or DA will be required to change password after inputting his/ her User ID and the expired password at the login page.

2 Password Reset

Enabled mobile app OTP



b

Self-served by Forgot/ Reset Password function

Enabled email OTP



c

For DAs: submit eService DA 3 by Client Connect user
For users: Unlock/ Reset OTP Device Registration by DA

3 Change mobile device

d

Self-served by Authentication Settings function

8. Appendix 1 – Account Maintenance for Users and DAs (Cont'd)

Type of Account Maintenance

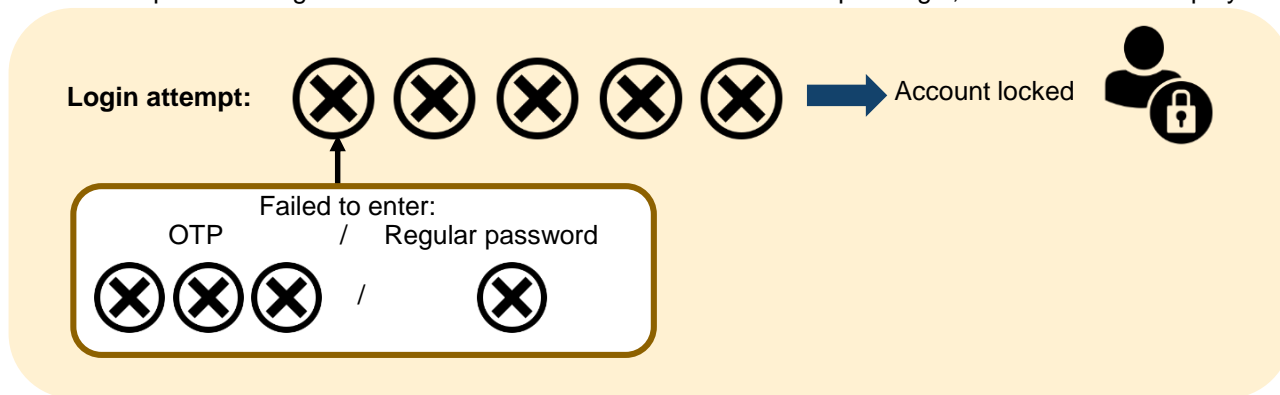
Action Required

4 Unlock Account

c

For DAs: submit eService DA 3 by Client Connect user
For users: Unlock/ Reset OTP Device Registration by DA

- DA's and User's access will be locked after 5 consecutive unsuccessful attempts of login, while 3 consecutive unsuccessful attempt of entering OTP will be counted to 1 unsuccessful attempt of login, an illustration is displayed below:



8. Appendix 1 – Account Maintenance for Users and DAs (Cont'd)

a

Self-served by Change Password function

1 After logging into CCASS/ CCMS or DMS

Click <Change Password>

CCASS/ CCMS

DMS

Change Password

2 A pop-up page will be displayed

HKEX 香港交易所 AUTHENTICATION SETTINGS

Change password

Enter new password twice, then click <Update>

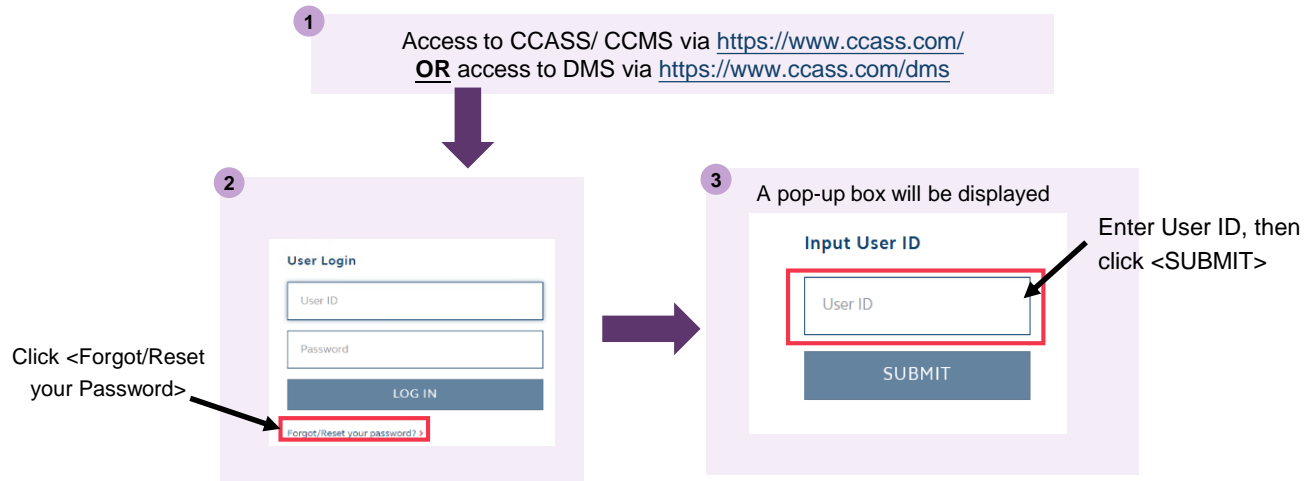
3 DA and user should enter the new password for accessing to CCASS/ CCMS or DMS in the next login.

Completed

8. Appendix 1 – Account Maintenance for Users and DAs (Cont'd)

b

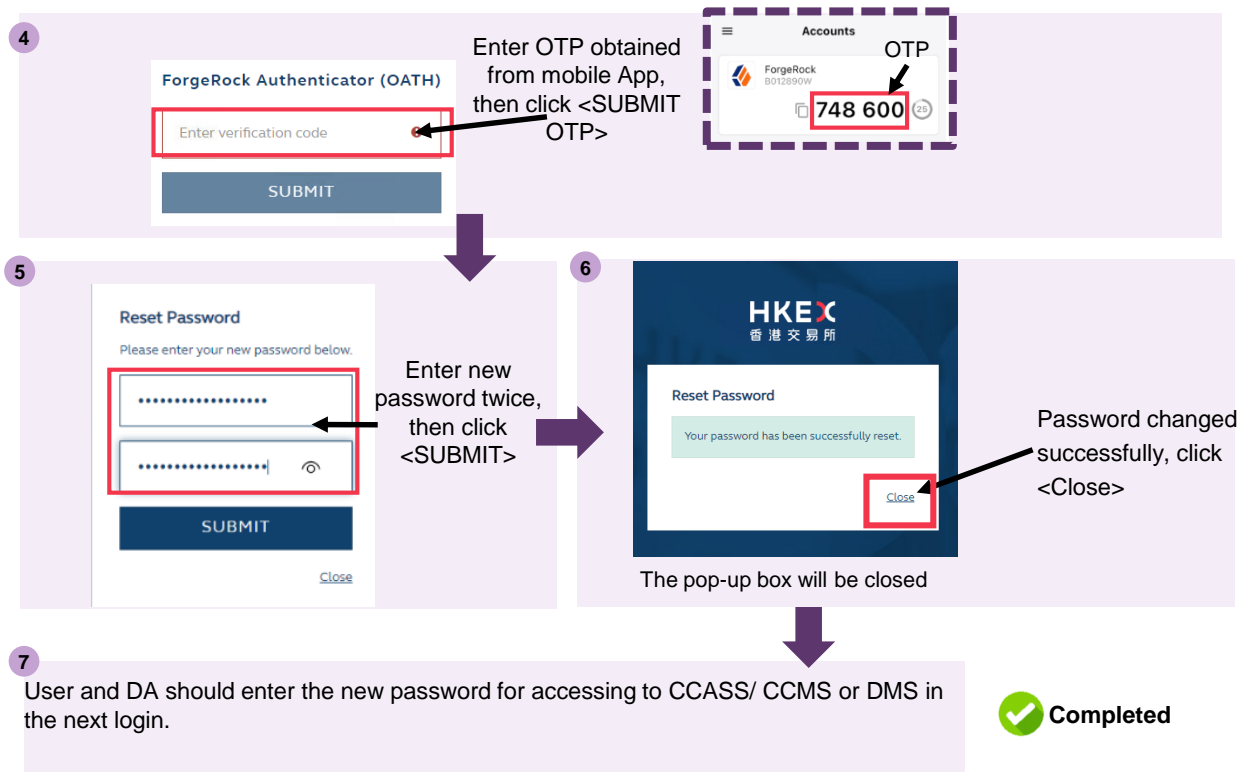
Self-served by Forgot/ Reset Password function



8. Appendix 1 – Account Maintenance for Users and DAs (Cont'd)

b

Self-served by Forgot/ Reset Password function (cont'd)



8. Appendix 1 – Account Maintenance for Users and DAs (Cont'd)

c

For DAs: submit eService DA 3 by Client Connect user

To be Performed by Client Connect Maker and Checker

- 1 Submit eService DA3 in Client Connect through HKEX Access Management Portal.

Enter User ID and
the registered email
address of user

DETAILS OF REQUESTS

DETAILS OF UNLOCK / ENABLE / DISABLE REQUEST

User ID
Type your answer here...

Email Address
Type your answer here...

+ REQUEST

Remarks
Type your answer here...

Please Choose

Unlock DA Account

Unlock DA Account

Enable DA Status

Disable DA Status

Select <Unlock DA
Account>

A system generated email notification will be available upon the completion of the request

2

In the next login, DA will need to carry out both “Set up password” and “Set up OTP Channel” procedure as if first time login.



Completed



8. Appendix 1 – Account Maintenance for Users and DAs (Cont'd)

c

For users: Unlock/ Reset OTP Device Registration by DA

To be performed by DA Maker

1 After logging into DMS

Click <Maintain User Profile>, then click <Change User Profile>

2

User Profile Print Site Map Logout Change Password DUPC 01 15-Apr-23 12:56:56

Change User Profile - Prompt

User ID Submit Enter User ID and click <Submit>

Search by ☐ User ID ☐ User Name

Search Filter *

List Refresh

3

Change User Profile - Detail

This is an end-user profile

Organisation	B01281
Internal/External	EXTER
User ID	B01281
User Status	<input checked="" type="radio"/> EN <input type="radio"/> DI
Surname	EU01
Other Names	EU01
Email	osss_eu1@hkex.com.hk
Enable From	<input type="text"/> DDMMYY
Disable After	<input type="text"/> DDMMYY
Locked	No <input checked="" type="radio"/> Yes
OTP Enabled	Yes
Cleaning House Options	Cash
Access Channel	C3T

Click the radio button of <Unlock/ Reset OTP Device Registration>

Then click <Change>

Change Refresh

8. Appendix 1 – Account Maintenance for Users and DAs (Cont'd)

c

For users: Unlock/ Reset OTP Device Registration by DA (cont'd)

To be performed by DA Checker

4 Redirected to the confirmation page

Change User Profile - Confirmation

This is an end-user profile

Organisation	B01289 SOUTH CHINA SECURITIES LTD
Internal/External	EXTERNAL
User ID	B012890W
User Status	ENABLED
Surname	EU01
Other Names	EU01
Email	osaa_eur1@hkes.com.hk
Enable From	
Disable After	
Locked	No Will Unlock/Reset OTP Device Registration
OTP Enabled	Yes
Clearing House Options	Cash
Access Channel	CST
Transaction limit (HKD)	
Default	0.00
DI	
ISI	
Cash Compensation Indicator	
Cash Prepayment	

DI Requirement	
Recall Request	
ATI	
SI	

Checker ID

Authorisation Code

Confirm

Back

Enter Checker ID
and Authorization
Code, then click
<Confirm>

Confirmation message will be
displayed on the bottom of the page

THE ABOVE USER PROFILE IS CHANGED SUCCESSFULLY

5 In the next login, user will need to carry out both “Set up password” and “Set up OTP Channel” procedure as if first time login.

✓ Completed



8. Appendix 1 – Account Maintenance for Users and DAs (Cont'd)

d

Self-served Authentication Settings function

1 After logging into CCASS/ CCMS or DMS

Click <Change Password>

CCASS/ CCMS

DMS

Change Password

Change Password

2 A pop-up page will be displayed

Click <AUTHENTICATION SETTINGS>

Change password

Password

New password

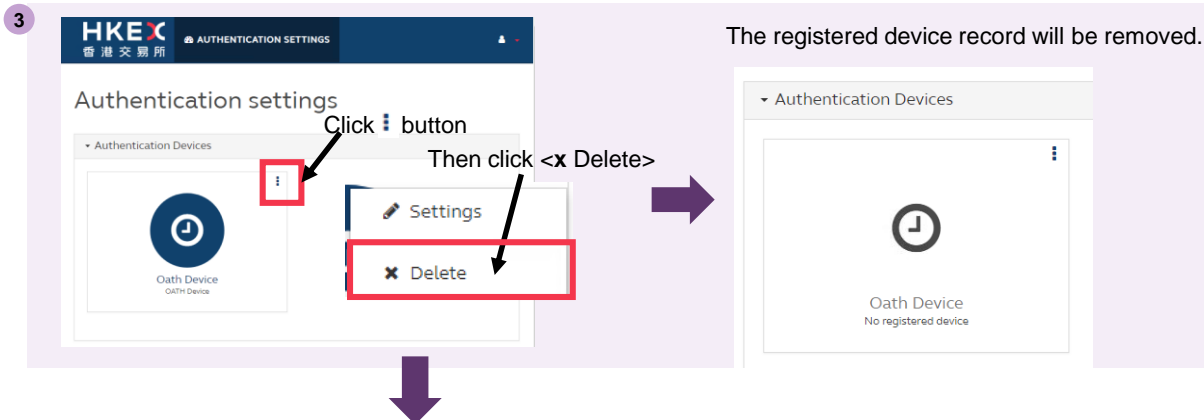
Confirm new password

Reset Update

8. Appendix 1 – Account Maintenance for Users and DAs (Cont'd)

d

Self-served Authentication Settings function (cont'd)



- 4 In the next login, user or DA will need to carry out “Set up OTP Channel” procedure to register another mobile device.

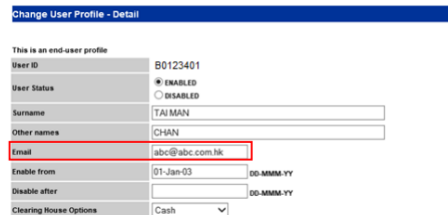
✓ Completed


8. Appendix 2 – Procedure of Email Registration for Users and DAs

Upon the launch of 2FA, users are required to setup their regular password to initiate the 2FA. An OTP email will be sent to users designated email address for authentication. Therefore, it is important for users to register their designated email addresses in advance.

1. Register designated email address for CCASS/ CCMS users

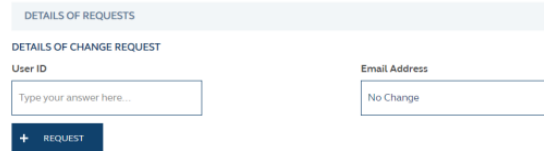
- ❑ CCASS/ CCMS DAs who perform the user profile maintenance functions shall register the designated email address of their users in DMS





The updated user profile shall be effective shortly upon the completion of maker-checker process.

2. Register designated email address for CCASS/ CCMS DAs

- ❑ Client Connect user with access right “EU_UserMaintenance” shall register the designated email address of the CCASS/ CCMS DAs by submitting eService DA3 <CCASS/ CCMS Delegated Administrator Application/ Maintenance Form> in Client Connect through HKEX Access Management Portal




HKEX will process eService request by batch, and will start processing of eServices submitted before 28 April 2023 during late-Apr – May 2023.



CPs and DBs must register the designated email addresses of their CCASS/ CCMS users and DAs before 28 April 2023 (Friday) to initialize 2FA for accessing to CCASS/ CCMS at the launch of 2FA.

8. Appendix 2 – Procedure of Email Registration for Users and DAs (Cont'd)

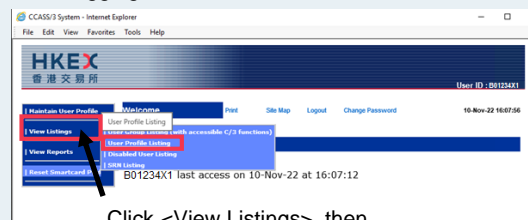
User ID can be found in DMS:

- through “User Profile Listing” Function

To be performed by DA

1

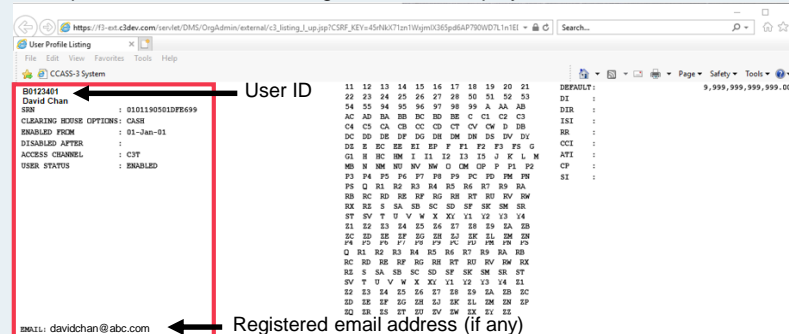
After logging into DMS



Click <View Listings>, then
click <User Profile Listing>

2

The profile of all users including DAs will be displayed



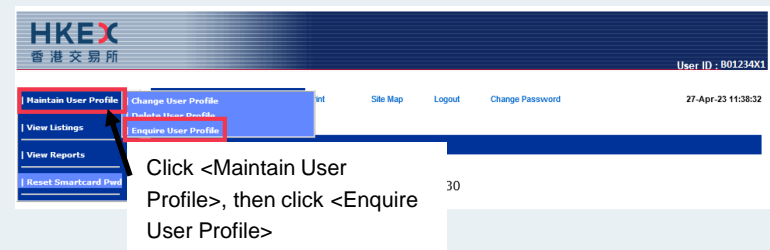
8. Appendix 2 – Procedure of Email Registration for Users and DAs (Cont'd)

User ID can be found in DMS:

- through “Enquire User Profile” Function

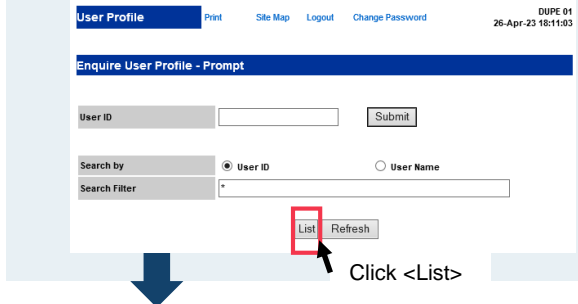
To be performed by DA

1 After logging into DMS



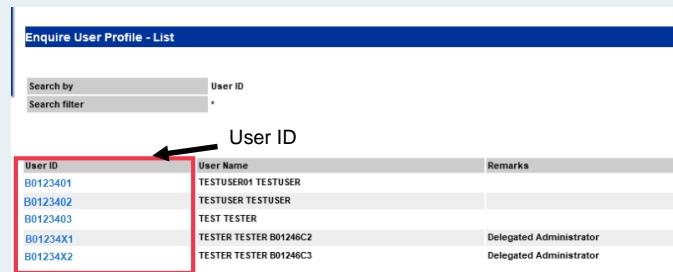
Click <Maintain User Profile>, then click <Enquire User Profile>

2



Click <List>

3 The User ID and the corresponding User Name will be displayed



User ID	User Name	Remarks
B0123401	TESTUSER01 TESTUSER	
B0123402	TESTUSER TESTUSER	
B0123403	TEST TESTER	
B01234X1	TESTER TESTER B01246C2	Delegated Administrator
B01234X2	TESTER TESTER B01246C3	Delegated Administrator

8. Appendix 2 – Procedure of Email Registration for Users and DAs

Email Registration for Users

To be performed by DA Maker

1

Access to DMS via <https://www.ccass.com/dms>

2

Enter smartcard password, then click <Logon>

3

Click <Maintain User Profile>, then click <Change User Profile>

4

Enter User ID, then click <Submit>

5

Enter email address of the user

Then click <Change>

8. Appendix 2 – Procedure of Email Registration for Users and DAs (Cont'd)

Email Registration for Users (Cont'd)

To be performed by DA Checker

6

On the same page

Change User Profile - Confirmation

This is an end-user profile

User ID	B0124601
User Status	ENABLED
User name	TAI MAN CHAN
Email	abc@abc.com.hk
Enable from	01-Jan-03
Disable after	
Clearing House Options	Cash
Transaction limit (HKD)	
Default	9,999,999,999,999.99
DI	
ISI	
Cash Compensation Indicator	
Cash Prepayment	
DI Requirement	
Recall Request	
ATI	
SI	

Selected User Groups

11 12 13 14 15 16 17 18 19 20 21 22 23
24 51 52 54 55 A AA AB AC AD C CH D
DV DX E F F1 H I J K L M N NU NV
O P PD PM Q R RA RB RD RU RX RY RZ
SA SM ST WA WB WC WD WE WF WG

Checker ID B01246X2

Authorisation Code *****

Confirm Back

Enter <Checker ID> and <Authorization Code>, then click <Confirm>

Confirmation message will be displayed on the bottom of the page

THE ABOVE USER PROFILE IS CHANGED SUCCESSFULLY

✓ Completion of email registration for user



8. Appendix 2 – Procedure of Email Registration for Users and DAs (Cont'd)

To be performed by Client Connect Maker

Email Registration for DAs

1

Access to HKEX Access Management Portal via
<https://connect.hkex.com.hk/>

2

Enter Email and Password, then click <LOG IN>

3

Click <Partnership Management>, then click <User Maintenance> and then <CCASS/ CCMS Delegated Administrator Application/ Maintenance Form>

Classification	ID	Function	Format	Reference
User Maintenance CC	SCard2	Smartcard Maintenance for User (PG or Special Request)		
User Maintenance CH	SCard1	Smartcard Maintenance for User and DA		
User Maintenance CH	SCard3	Order Smartcard Renewal		
User Maintenance CC	DA.3	CCASS/ CCMS Delegated Administrator Application/ Maintenance Form		

4

Reference Number: Status: Expand

COMPANY INFORMATION

From
ABC Company

As

- ☒ HKSCC Participant (B01234)
- ☐ HKCC Participant (XYZ)
- ☐ SEIOCH Participant (XYZ)

MAINTENANCE REQUEST

Maintenance Request
☒ Change

Maintenance Request will be selected as "Change" by default

8. Appendix 2 – Procedure of Email Registration for Users and DAs (Cont'd)

To be performed by Client Connect Maker

Email Registration for DAs (Cont'd)

5 Enter User ID and the designated email address of DA

DETAILS OF REQUESTS

DETAILS OF CHANGE REQUEST

User ID
B01234X1

Email Address
ABC@bank.com.hk

+ REQUEST

Remarks
Type your answer here.

If necessary, click <+ Request> to register email address for other DAs (max 4 DA's profile can be updated under 1 eService>

We declare that the information provided in this eService relating to us is complete, true and correct and that we have not made any statements or omissions which are misleading or false in any material particular.

☒ We confirm that we understand and accept the above.

Tick the declaration box

6 Check if Contact Information is correct

CONTACT INFORMATION

Name of Contact Person
AAA

Email Address
AAA@bank.com.hk

Telephone Number
29797111

+ CONTACT PERSON

7

Home /

SAVE PREVIEW

DA 3 CCASS/ CCMS DELEGATED ADMINISTRATOR APPLICATION/ MAINTENANCE FORM

Reference Number:

Status: ☒ Expand

8. Appendix 2 – Procedure of Email Registration for Users and DAs (Cont'd)

To be performed by Client Connect Maker

Email Registration for DAs (Cont'd)

Click <Submit, then click <Confirm>

The screenshot shows a web form titled "DA 3 CCASS/ CCMS DELEGATED ADMINISTRATOR APPLICATION/ MAINTENANCE FORM". At the top, there are buttons for "DISCARD", "EDIT", and "SUBMIT". The "SUBMIT" button is highlighted with a red box and a red circle with the number "1". An arrow points from the "SUBMIT" button to a confirmation dialog box. The dialog box has a title "PLEASE CONFIRM" and a subtitle "PROCEED". It contains the text: "The record will be ready to send to HKEX. Any message to the next step user? (Optional)". At the bottom of the dialog, there are "CANCEL" and "CONFIRM" buttons. The "CONFIRM" button is highlighted with a red box and a red circle with the number "2". An arrow points from the "CONFIRM" button back to the main form.

The eService request status will be changed from "Draft" to "Ready to Send to HKEX", the eService Reference Number is generated.

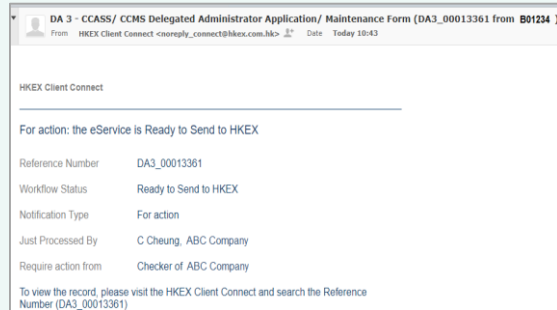
The screenshot shows the same web form as above, but now the status is "Ready to Send to HKEX" and a reference number has been generated. The "RECLAIM" button is highlighted with a red box. The "CLONE" button is also visible. The Reference Number is "DA3_00013361" and the Status is "07-Feb-2023 10:43 HKT Ready to Send to HKEX".

9. Appendix 2 – Procedure of Email Registration for Users and DAs (Cont'd)

Email Registration for DAs (Cont'd)

To be performed by Client Connect Checker

A system generated email notification with the eService Reference Number will be sent to checker's email upon submission of maker's request.



DA 3 - CCASS/ CCMS Delegated Administrator Application/ Maintenance Form (DA3_00013361 from B01234)

From: HKEX Client Connect <ourghly_connect@hkex.com.hk> Date: Today 10:43

HKEX Client Connect

For action: the eService is Ready to Send to HKEX

Reference Number: DA3_00013361

Workflow Status: Ready to Send to HKEX

Notification Type: For action

Just Processed By: C Cheung, ABC Company

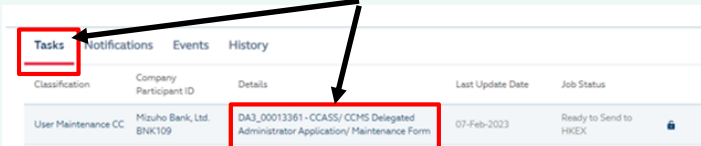
Require action from: Checker of ABC Company

To view the record, please visit the HKEX Client Connect and search the Reference Number (DA3_00013361)

9

Access to HKEX Access Management Portal

Click <Tasks>, then click the appropriate reference number



Classification	Company Participant ID	Details	Last Update Date	Job Status
User Maintenance CC	Mizuho Bank, Ltd. BNK109	DA3_00013361 - CCASS/ CCMS Delegated Administrator Application/ Maintenance Form	07-Feb-2023	Ready to Send to HKEX

10

Click <Claim>



Home /

CLAIM

DA 3 CCASS/ CCMS DELEGATED ADMINISTRATOR APPLICATION/ MAINTENANCE FORM

Reference Number: DA3_00013361 Status: 07-Feb-2023 10:43 HKT Ready to Send to HKEX Expand

COMPANY INFORMATION

8. Appendix 2 – Procedure of Email Registration for Users and DAs (Cont'd)

Email Registration for DAs (Cont'd)

To be performed by Client Connect Checker

Click <Confirm>, then click <Confirm>

Home /

REVERT REFER TO

Claimed By D Wong on 07-Feb-2023 10:45 HKT

CONFIRM RELEASE

DA 3 CCASS/ CCMS DELEGATED ADMINISTRATOR APPLICATION/ MAINTENANCE FORM

Reference Number: DA3_00013361 Status: 07-Feb-2023 10:43 HKT Ready to Send to HKEX | Expand

PLEASE CONFIRM TO PROCEED

The record will be sent to HKEX.

Any message to the record user? (optional)

CANCEL **CONFIRM**

The request status will be changed from “Ready to Send to HKEX” to “Sent to HKEX”.

Home /

RECLAIM

DA 3 CCASS/ CCMS DELEGATED ADMINISTRATOR APPLICATION/ MAINTENANCE FORM

Reference Number: DA3_00013350 Status: 07-Feb-2023 10:43 HKT Sent to HKEX | Expand

After HKEX completed processing the eService, a system generated email notification will be available.

DA 3 - CCASS/ CCMS Delegated Administrator Application/ Maintenance Form (DA3_00013361 from 801234)

From: HKEX Client Connect <coreply_connect@hkex.com.hk> Date: Mon 18:29

HKEX Client Connect

For reference: the eService is Completed

Reference Number: DA3_00013361

Workflow Status: Completed

Notification Type: For reference

Just Processed By: HKEX

Require action from: Nil

To view the record, please visit the HKEX Client Connect and search the Reference Number (DA3_00013361).

You may visit the record to download a PDF version of the eService for reference if needed.



Completion of email registration for DA

Disclaimer

The information contained in this presentation is for general informational purposes only and does not constitute an offer, solicitation, invitation or recommendation to subscribe for or purchase any securities or other products or to provide any investment advice of any kind. This presentation is not directed at, and is not intended for distribution to or use by, any person or entity in any jurisdiction or country where such distribution or use would be contrary to law or regulation or which would subject Hong Kong Exchanges and Clearing Limited ("HKEX") to any registration requirement within such jurisdiction or country.

This presentation contains forward-looking statements which are based on the current expectations, estimates, projections, beliefs and assumptions of HKEX about the businesses and the markets in which it and its subsidiaries operate or aspires to operate in. These forward-looking statements are not guarantees of future performance and are subject to market risk, uncertainties and factors beyond the control of HKEX. Therefore, actual outcomes and returns may differ materially from the assumptions made and the statements contained in this presentation. The implementation of these initiatives is subject to a number of external factors, including government policy, regulatory approval, the behaviour of market participants, competitive developments and, where relevant, the identification of and successful entry into agreements with potential business partners. As such, there is no guarantee that the initiatives described herein will be implemented, or that they will be implemented in the form and timeframe described herein.

Although the information contained in this presentation is obtained or compiled from sources believed to be reliable, HKEX does not guarantee the accuracy, validity, timeliness or completeness of the information or data for any particular purpose, and shall not accept any responsibility for, or be liable for, errors, omissions or other inaccuracies in the information or for the consequences thereof. The information set out in this presentation is provided on an "as is" and "as available" basis and may be amended or changed. It is not a substitute for professional advice which takes account of your specific circumstances and nothing in this document constitutes legal advice. HKEX shall not be responsible or liable for any loss or damage, directly or indirectly, arising from the use of or reliance upon any information provided in this presentation.

