Changes in relation to the implementation of Two-Factor Authentication (2FA) for Terminal access to CCMS are shaded in orange for ease of reference.

Getting Started For Terminal Operations

ACCESS CONTROL

INTRODUCTION:

This section details the access control of CCMS. The account maintenance of the delegated administrators (DAs) of the Participants including assignment of DAs' user ID is centralised and administered by HKEX, while the DAs are responsible for maintaining the user profile of the users, including the assignment of their users' user IDs. Please refer to section 3.2 on Security Management.

Access controls are implemented to ensure that only relevant CCMS information is accessible to authorised users (users). It is achieved through the following elements:

- Two-Factor Authentication (2FA)
- smartcard
- Participant ID
- user profile, which includes:
  - user ID
  - user access level assignment
- IP address
- inactivity timeout

1. Two-Factor Authentication (2FA)

A Participant may delegate his CCMS operations to a number of users. To establish a new user, a Participant will need to apply to HKSCC by submitting the eService Form – DA 4 "CCASS / CCMS User Account Application Form" (as stated under "HKEX Website"). It should be noted that each user account is unique to that assigned user, and cannot be shared by other users or Participants.

Upon the implementation of 2FA for Terminal access to CCMS, all new users and DAs created can only access to CCMS by 2FA. Each user and DA of the Participant must logon CCMS Terminal by their user ID, password and One-Time-Password (OTP) obtained from the designated channel (i.e. mobile application or email).

Users and DAs must initialise 2FA by setting up a password according to the HKEX Password Policy and the designated channel to obtain OTP when he/she first logs on CCMS through the CCMS Terminal. For details, please refer to Section 3.4 on LOGON AND LOGOFF CCMS.

User's access will be locked after 5 consecutive unsuccessful attempts of login within 30 minutes, while 3 consecutive unsuccessful attempts of entering OTP will be counted as 1 unsuccessful attempt of login. Please refer to Section 3.6 on ACCOUNT MAINTENANCE.

2. Smartcard:

The smartcard authentication method for Terminal access of CCMS will remain until the decommissioning on 4 September 2023 (Monday) tentatively.

Users remain accessing to CCMS by smartcard, must insert his/her smartcard into the smartcard reader connecting to a CCMS Terminal and input a correct smartcard password in order to logon to CCMS.

3. Participant ID:

For Cash Participants (HKSCC):

HKSCC assigns a Participant ID to each Participant when he/she is admitted into CCASS. It is a six-character code (e.g. B12345) consisting of a one-digit prefix and five-digit serial number. The prefix indicates the participant nature (B for Clearing Participants which are also Exchange Participants of SEHK; A for Clearing Agency Participants; C for Custodian Participants / Clearing Participants which are not Exchange Participants of SEHK, e.g. registered institutions; L for Stock Lender Participants; P for Stock Pledgee Participants; and numeric number for investor). CCASS Participants have the same Participant ID to access both CCASS and CCMS.

For Derivatives Participants (HKCC and SEOCH):

HKCC or SEOCH assigns a Participant ID to a Participant when he/she applies to access CCMS. It is a six-character code. For derivatives participants, the code is defined as HKXXXn, where:

XXX = a unique mnemonic assigned to represent the participant (normally same as the one in DCASS)
n = 1 for HKCC participants, and 2 for SEOCH participants

Example: HKABC1. This would be participant "ABC" of HKCC.

4. User ID:

A unique user ID is assigned to each user and DA of a Participant. HKEX shall assign user ID for each DA of the Participant, while DAs shall assign user ID for their users. It is an eight-character code (e.g. HKABC101 for Derivatives Participants or B1234501 for Cash Participants), of which the first six characters are identical to the Participant ID. HKEX has the right to suspend or delete any user ID of a Participant.

5. User Access Level Assignment:

CCMS users can only access pre-authorised CCMS functions. Due to the job nature of individual user and internal control consideration (e.g., operator as maker, manager as checker, etc.), a CCMS user may only be allowed to access relevant CCMS functions (e.g., data entry functions for operators, and authorisation functions for managers).

CCMS functions are grouped into different categories, called User Access Group. Participants are recommended to assign appropriate combinations of the User Access Groups to each of the users as his/her user access level through its DAs, by considering segregation of duties for internal control. Participant may alter the User Access Level of its CCMS users at any time

through its DAs. If a CCMS user attempts to use an unauthorised function, an error message will be displayed. Please refer to Table 3.1.1 for the definition of CCMS user access groups.

TABLE 3.1.1 - CCMS USER FUNCTIONS

CCMS FUNCTIONS	USER ACCESS LEVEL CODE											
	P	Q	S	T	U	W	X	BA	BB	BC	BD	BE
GENERAL FUNCTIONS												
Enquire Broadcast Message	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓
Report Download											✓	
Report Profile Maintenance											✓	
STOCK TRANSFER FROM/TO CCASS												
Add CCASS-To-CCMS Stock Transfer	✓											
Add CCMS-To-CCASS Stock Transfer					✓							
Add General to Specific Stock Collateral		✓										
Add Specific to General Stock Collateral				✓								
COLLATERAL DEPOSIT												
Add Cash Collateral Deposit Order									✓			
Delete Cash Collateral Deposit Order									✓			
Authorise Cash Collateral Deposit Order										✓		
Add Non-Cash Collateral Deposit Order									✓			
Delete Non-Cash Collateral Deposit Order									✓			
Authorise Non-Cash Collateral Deposit Order										✓		
Enquire Deposit or Withdrawal Order									✓	✓		
COLLATERAL WITHDRAWAL												
Add Cash Collateral Withdrawal Order									✓			
Delete Cash Collateral Withdrawal Order									✓			
Authorise Cash Collateral Withdrawal Order										✓		
Add Non-Cash Collateral Withdrawal Order									✓			
Delete Non-Cash Collateral Withdrawal Order									✓			
Authorise Non-Cash Collateral Withdrawal Order										✓		
Enquire Deposit or Withdrawal Order									✓	✓		
PARTICIPANT SUBMITTED DEPOSIT/ WITHDRAWAL ORDER												
Reject Submitted Cash Collateral Deposit/ Withdrawal Order										✓		
COLLATERAL TRANSFER												
Add Cash Collateral Account Transfer Instruction									✓			
Delete Cash Collateral Account Transfer Instruction									✓			

CCMS FUNCTIONS	USER ACCESS LEVEL CODE											
	P	Q	S	T	U	W	X	BA	BB	BC	BD	BE
Authorise Cash Collateral Account Transfer Instruction										✓		
Enquire Cash Collateral Account Transfer Instruction									✓	✓		
Add Non-Cash Collateral Account Transfer Instruction									✓			
Delete Non-Cash Collateral Account Transfer Instruction									✓			
Authorise Non-Cash Collateral Account Transfer Instruction										✓		
Enquire Non-Cash Collateral Account Transfer Instruction									✓	✓		
SPECIFIC CASH COLLATERAL												
Add Pending Specific Cash Collateral						✓						
Delete Pending Specific Cash Collateral						✓						
Authorise Pending Specific Cash Collateral							✓					
Enquire Specific Cash Collateral						✓	✓					
PREFERRED SINGLE SETTLEMENT CURRENCY												
Change Preferred Single Settlement Currency						✓						
Delete Pending Preferred Single Settlement Currency						✓						
Authorise Pending Preferred Single Settlement Currency							✓					
Enquire Preferred Single Settlement Currency						✓	✓					
ENQUIRE COLLATERAL INFORMATION												
Enquire Collateral Account												✓
Enquire Collateral Account To Transaction Account Relationship												✓
Enquire Collateral Account Balance			✓									✓
Enquire Collateral Account Movement			✓									✓
Enquire Collateral Inventory			✓									✓
Enquire Interest Calculation Result / Accommodation Fee			✓									✓
Enquire Currency Exchange Rate and Haircut			✓									✓
Enquire Collateral Effective Haircut & Valuation Price			✓									✓
Enquire Specific Cash Collateral Movement			✓									

'✓' means the user has the access right to the functions.
HKSCC Participants can apply user groups P, Q, S, T, U, W and X.
HKCC Participants can apply user groups BA, BB, BC, BD and BE.
SEOCH Participants can apply user groups U, BA, BB, BC, BD and BE.

TABLE 3.1.2 - DELEGATED ADMINISTRATOR FUNCTIONS

SECURITY MANAGEMENT FUNCTIONS	USER ACCESS LEVEL CODE EE
SECURITY MANAGEMENT	
Enquire User Profile	✓
View User Group Listing (with accessible C/3 functions)	✓
View User Profile Listing	✓
View Disabled User Listing	✓
View SRN Listing	✓
View User Profile Maintenance Report	✓

'✓' means the user has the access right to the functions.

6. IP address :

When a Participant set up a CCMS Terminal, HKEX will assign an IP address (Internet Protocol) for configuration into the computer. HKEX maintains the relationship of IP addresses and their relevant Participants, and will deny access attempts from PCs with unrecognised IP addresses.

7. Inactivity timeout:

CCMS is automatically logged off if the user or DA does not operate at the terminal for a certain time period (about 15 minutes). To access CCMS again, the user or DA has to close the browser and perform the logon procedures. This prevents other unauthorized persons from using the CCMS Terminal if a CCMS user or DA forgets to logoff from CCMS. Please refer to Section 3.4 for further details on inactivity timeout.

8. Participants' security responsibility

Each Participant is responsible for establishing and informing HKEX of subsequent changes to the list of authorised signatories to approve various request forms regarding CCMS DAs and other matters in relation to CCMS access.

It is the responsibility of each Participant to control access to its CCMS Terminal and to the users' and DAs' designated OTP channel and smartcards (where applicable) to ensure the security and confidentiality of the user IDs and passwords, and smartcard passwords (where applicable) of its assigned users and DAs, to ensure that the users' account are associated with appropriate Access Levels for segregation of duties and its assigned users abide by the Access Levels assigned to each of them, to ensure the security and confidentiality of the Authorisation Code (detailed in Section 3.2) of its DAs, and to ensure that its DAs abide by the Administrator Rights assigned to them.

For 2FA users and DAs, in case of lost of password, they can perform self-service password reset if they have enabled mobile application to obtain OTP, given that their account is not locked. If they have enabled email to obtain OTP, DA should perform Unlock/ Reset OTP Device Registration in DMS for their users to reset password, while Participant shall immediately notify HKEX to Unlock/ Reset OTP Device Registration for its DA by submitting to

HKEX the eService Form – DA 3 “CCASS/ CCMS Delegated Administrator Application/ Maintenance Form” (as stated under “HKEX Website”).

For smartcard users and DAs, in case of lost of smartcard, DA should disable the user profile for their users in DMS, while Participant shall immediately notify HKEX to disable the user profile of its DA by submitting to HKEX the eService Form – DA 3 “CCASS/ CCMS Delegated Administrator Application/ Maintenance Form” (as stated under “HKEX Website”). Users and DAs will need to adopt 2FA to access CCMS Terminal after enabling the user profile. Smartcard and Smartcard Reader are no longer available for purchase.

Participants shall be liable for all instructions input into CCMS via their CCMS Terminals. Participants requiring additional user account must submit to HKEX the eService Form – DA 4 “CCASS/ CCMS User Account Application Form” (as stated under “HKEX Website”). Participants are required to pay the appropriate fees for additional user account(s) as stipulated in the clearinghouses' Rules and Operational Procedures.