Getting Started For Terminal Operations

SECURITY MANAGEMENT

The user profile maintenance functions will be primarily performed by the participants. HKSCC shall assign a unique user ID for each delegated administrator (DA) of the Participant, while DA shall assign user IDs for their users. Each Participant should assign at least three delegated administrators (DAs), including one DA maker and two DA checkers, acting separately to perform the user profile maintenance functions including create, change and delete user profile. Please refer to table 3.2.1 for the full list of security functions.

To appoint a DA, a Participant must submit to HKSCC the eService Form – DA 3 "CCASS / CCMS Terminal Delegated Administrator Application/ Maintenance Form" (as stated under "HKEX Website"). Upon receipt of the valid form, HKSCC will provide to the Participant concerned a unique user ID for the DA. The Participant must ensure that its DA setup his password and the designated channel to obtain One-Time-Password (OTP) immediately upon receipt of the user ID. Please refer to Section 3.3 for detail procedures.

The Security Management functions are accessible via a separate URL ***https://www.ccass.com/dms***. The logon procedures for the Security Management are basically the same as those for accessing other functions. Please refer to Section 3.4 for the detail procedures. However, the user should type ***https://www.ccass.com/dms*** instead of the CCASS URL in the box next to the address field in step 4 in sub-section A LOGON CCASS.

Table 3.2.1 lists the CCASS functions and reports related to Security Management transactions.

TABLE 3.2.1: Functions and reports related to Security Management transactions

	CCASS Functions	**Section in this User Guide**
Terminal operation functions	• User Profile Maintenance • Get Authorisation Code	Section 8.4.1 Section 8.4.7
Reports	• User Group Listing (With Accessible Functions) • User Profile Listing • Disabled User Listing • User Profile Maintenance Report *The above reports are available for retrieval through the Security Management.*	Section 8.4.2 Section 8.4.3 Section 8.4.4 Section 8.4.6

Table 3.2.2 summarise the administration rights that can be assigned to the DAs regarding the Security Management functions to be performed by Participants.

TABLE 3.2.2: Administration rights related to Security Management transactions

Administration Rights	**Function**	**Remarks**
Maintain User Profile	• Create User Profile Input user name, email address, transaction limits and user groups and assign user ID	Given that there is available user accounts. Maker-checker mechanism is provided.
	• Change User Profile Input / modify user name and email address, input transaction limits and user groups; unlock, enable or disable a user profile	Maker-checker mechanism is provided.
	• Delete User Profile	
	• Enquire User Profile	
	• Get Authorisation Code	For enquiry of the authorisation code by checker.
	View Listings • User Group Listing (With Accessible Functions) • User Profile Listing • Disabled User Listing	
	View Report • User Profile Maintenance Report	