Getting Started For Terminal Operations

SECURITY MANAGEMENT

The user profile maintenance functions will be primarily performed by the Designated Banks. HKSCC will distribute smartcards to the Designated Banks and assign a user ID for each of the smartcards. Each Designated Bank should assign at least two delegated administrators (DAs), acting separately as a maker and a checker to perform the user profile maintenance functions including change and delete of user profiles and reset smartcard passwords. Please refer to table 3.2.1 for the full list of security functions.

To appoint and cancel the assignment of a DA, a designated bank must submit to HKSCC the eService Form – SCard 1 "Smartcard Maintenance for User and DA" (as stated under "HKEX Website"). Upon receipt of the valid form, HKSCC will provide to the designated bank concerned a unique User ID and smartcard for the DA. The designated bank must ensure that its DA creates or changes his initial Smartcard Password (where applicable) immediately upon receipt of the smartcard. 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 • Reset smartcard password • Get Authorisation Code	Section 7.3 Section 7.9 Section 7.10
Reports	• User Group Listing (With Accessible Functions) • User Profile Listing • Disabled User Listing • SRN Listing • User Profile Maintenance Report	Section 7.4 Section 7.5 Section 7.6 Section 7.7 Section 7.8

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

TABLE 3.2.2: Administration rights related to Security Management transactions

Administration Rights	**Function**	**Remarks**
Maintain User Profile	• Change User Profile Input / modify user name, input transaction limits and user groups; enable or disable a user	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 • SRN Listing #	
	View Report • User Profile Maintenance Report	
Reset Smartcard Password	• Reset smartcard password Smartcard password of authorised users only; not applicable to smartcard password of DA, which will be reset by HKSCC	• No maker-checker mechanism. • Can be a separate function performed by a different DA.
	• Enquire User Profile	
	View Listings • User Group Listing (With Accessible Functions) • User Profile Listing • Disabled User Listing • SRN Listing #	
	View Report • User Profile Maintenance Report	

#A List of the 'Subscriber Reference Number' encrypted in each smartcard issued to users and DA.