Getting Started for Terminal Operations

ACCESS CONTROL

INTRODUCTION:

This section details the access control of CCASS. The assignment of user ID is currently centralized and administered by HKSCC while the delegated administrators (DAs) of the designated banks are responsible for maintaining the user profile of the users. Please refer to section 3.2 on Security Administration Maintenance.

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

- ✓ smartcard
- ✓ designated bank ID
- ✓ user profile, which includes:
  - user ID
  - user access level assignment
- ✓ IP address
- ✓ inactivity timeout

1. Smartcard:

A designated bank must apply for the number of users that can access the CCASS functions and request for a smartcard for each of its users. A user must insert his/her smartcard into the smartcard reader connecting to a CCASS Terminal and input a correct smartcard password in order to logon to CCASS.

A smartcard reader will be required for each C3T installed. Designated Banks will need to apply smartcard readers by submitting to HKSCC the e-Service Form – SCard 3 “Order Smartcard Reader(s)” (as stated under “HKEX Website”).

A designated bank may delegate his CCASS operations to a number of internal staff ("CCASS users"). To establish a new CCASS user, a designated bank will need to apply to HKSCC by submitting the eService Form – SCard 1 “Smartcard Maintenance for User and DA” (as stated under “HKEX Website”). It should be noted that each smartcard is unique to that assigned CCASS user, and cannot be shared by other users or Designated Banks.

The CCASS user must initialise his/her smartcard by creating a smartcard password (6 - 8 digits) when he/she first logs on CCASS through the CCASS terminal. HKSCC recommends users to change their smartcard passwords periodically. Please refer to Section 3.3 on CHANGE SMARTCARD PASSWORD.

If a user enters an incorrect smartcard password for 3 consecutive times, the smartcard password will be revoked. The DA of the designated bank can reset the smartcard passwords of the users of the designated bank. Please refer to Section 7.3 on USER PROFILE MAINTENANCE.

2. Designated Bank ID:

Designated bank ID is assigned by HKSCC when a designated bank is admitted to CCASS. It is a six-character code beginning with 'BNK' (e.g. BNK024). The last three digits is the HKAB code of the bank.

3. User ID:

The designated bank must apply for the number of users that can access the CCASS functions. A unique user ID is assigned for each designated bank user by HKSCC. It is an eight-character code, of which the first six characters are identical to the designated bank ID (e.g. BNK02401). Although HKSCC cannot use the user ID for any CCASS function, it has the right to suspend or delete the user ID.

4. User Access Level Assignment:

Not all users can access every CCASS function. HKSCC has defined ten user levels by function availability: each user level can access a different set of CCASS functions. For example, users in some user levels (e.g. operators as makers) can access only the input functions while users in other user levels (e.g. managers as checkers) can access the authorization and enquiry functions. This helps the designated bank achieve segregation of duties for internal control.

TABLE 3.1: User access levels for designated bank users

Function Name	User Access Level Code										
	51	52	53	54	55	94	95	96	97	98	99
Input DDI/DCI/EPI Rejection	✓		✓						✓		✓
Delete DDI/DCI/EPI Rejection	✓		✓						✓		✓
Authorise DDI/DCI/EPI Rejection		✓	✓							✓	✓
Enquire DDI/DCI/EPI Rejection	✓	✓	✓						✓	✓	✓
Report Download	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Enquire Broadcast Message	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Input Rejected IP DDI/EPI						✓		✓	✓		✓
Delete Rejected IP DDI/EPI						✓		✓	✓		✓
Authorise Rejected IP DDI/EPI List							✓	✓		✓	✓
Rejected IP DDI/EPI File Upload				✓							
Authorise Rejected IP DDI/EPI File Upload					✓						
Enquire Payment Instruction	✓	✓	✓			✓	✓	✓	✓	✓	✓
Enquire SSA Bank Account	✓	✓	✓			✓	✓	✓	✓	✓	✓
Enquire Cash Projection	✓	✓	✓			✓	✓	✓	✓	✓	✓

✓' means the user has the access right to the function

Please apply to HKSCC if the designated bank needs to access file upload access levels 54 and 55.

FUNCTION NAME	USER ACCESS LEVEL CODE EE
SECURITY MANAGEMENT	
Enquire User Profile	✓
View User Group Listing (with accessible 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 function

5. IP address:

HKSCC maintains IP addresses of the PCs that the designated banks will be used to access CCASS and will deny access attempt from PCs with unrecognised IP addresses.

6. Inactivity timeout:

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

7. Designated Banks' security responsibility

Each designated bank is responsible for establishing and informing HKSCC of subsequent changes to the list of authorised signatories to approve various request forms regarding smartcard readers, smartcards, CCASS users, DAs and other matters in relation to CCASS access.

It is the responsibility of each designated bank to control access to its C3Ts and to its smartcards to ensure the security and confidentiality of the User IDs and smartcard passwords of its assigned users and DAs, to ensure that its smartcards 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 ensures that its DAs abide by the Administrator Rights assigned to them.

A designated bank shall immediately notify HKSCC to disable the user profile associated with a smartcard by submitting to HKSCC the eService Form – SCard 1 "Smartcard Maintenance for User and DA" (as stated under "HKEX Website") if it is found that the smartcard is lost or has been stolen.

Designated banks shall liable for all instructions input into CCASS via their C3Ts. Designated Banks requiring a new smartcard or a replacement smartcard must submit HKSCC the eService Form – SCard 1 "Smartcard Maintenance for User and DA" (as stated under "HKEX Website"). Designated Banks are required to pay the appropriate fees for issuance or replacement of a smartcard as stipulated in the CCASS OP.