HKEX
香港交易所

CCASS Operational Procedures

Definitions

(b) When used in the Operational Procedures, the following expressions shall have the following meanings unless the context otherwise requires:

The definitions of "Smartcard Password" has been repealed.

Section 3
CCASS Terminals/CCASS Phone System/CCASS Internet System/ Participant Gateways/RMS

3.5 ACCESS CONTROL OF CCASS TERMINALS AND PARTICIPANT GATEWAYS

3.5.1 Logging on to CCASS

Each User ID provided by HKSCC is unique to the Authorised User or Delegated Administrator to whom it is issued. The identity of an Authorised User or a Delegated Administrator logging on to CCASS will be determined by HKSCC by reference to the User ID used.

In order to log on to CCASS via a CCASS Terminal, an Authorised User or a Delegated Administrator must use his User ID and user password.

In the event that an Authorised User is unsuccessful in logging on to CCASS via a CCASS Terminal, the Participant concerned will need to re-establish that person as an Authorised User through its Delegated Administrator via a CCASS Terminal.

In the event that a Delegated Administrator of a Participant is unsuccessful in logging on to CCASS via a CCASS Terminal, the Participant concerned will need to re-establish that person as a Delegated Administrator by applying in the prescribed manner to HKSCC.

In order to log on to CCASS via a Participant Gateway, an Authorised User of a Participant must:

(i) insert the Participant Gateway smartcard of that Participant into the smartcard reader of the Participant Gateway; and

(ii) enter the Participant Gateway Smartcard Password of that Participant into the Participant Gateway.

Each Participant Gateway smartcard provided by HKSCC is unique to the Participant to whom it is issued. The identity of a Participant logging on to CCASS via a Participant Gateway will be determined by HKSCC by reference to the Participant Gateway smartcard used.

Participants may apply to HKSCC for smartcard readers for their Participant Gateways in the manner as specified in the CCASS Terminal User Guide.

Participants may also apply to HKSCC for a Participant Gateway Smartcard Password reset by completing the prescribed request form and submitting the same to HKSCC.

3.5.5 Participants responsible for security

It is the responsibility of each Participant to control and ensure the security of the access to its CCASS Terminals, Participant Gateways and to its Participant Gateway smartcards to ensure the security and confidentiality of the User IDs and user passwords of its Authorised Users and Delegated Administrators and its Participant Gateway Smartcard Password, to ensure that its Authorised Users abide by the Access Levels and Input Transaction Limits assigned to each of them, to ensure the security and confidentiality of the Authorisation Code of its Delegated Administrators, and to ensure that its Delegated Administrators abide by the Administrator Rights assigned to them.

A Participant shall immediately notify HKSCC to disable the user profile associated with a Participant Gateway smartcard by submitting the prescribed form to HKSCC if it becomes aware that the smartcard is lost or has been stolen.

Participants shall be liable for all instructions input into CCASS via their CCASS Terminals or Participant Gateways. Participants requiring a new Participant Gateway smartcard or a replacement Participant Gateway smartcard must complete the prescribed Smartcard Request Form and submit the same to HKSCC. Participants are required to pay the relevant fees relating to Participant Gateways and CCASS Terminals.