

An Overview of CCASS/3

May 2010

Table of Contents

| | |
|--|----------|
| A. WHAT IS CCASS/3 ? | 1 |
| B. CCASS/3 SERVICES..... | 1 |
| CLEARING AND SETTLEMENT SERVICES | 1 |
| DEPOSITORY AND NOMINEE SERVICES..... | 1 |
| COLLATERAL MANAGEMENT SERVICES | 1 |
| INVESTOR ACCOUNT SERVICES | 2 |
| STOCK SEGREGATED ACCOUNT WITH STATEMENT SERVICES | 2 |
| C. CCASS/3 TECHNOLOGY INFRASTRUCTURE | 2 |
| CCASS/3 TERMINAL..... | 3 |
| PARTICIPANT GATEWAY | 4 |
| NETWORK COMMUNICATION LAYER | 4 |
| SECURITY MEASURES | 4 |

A. What is CCASS/3 ?

CCASS/3 is a new generation of the Central Clearing And Settlement System implemented by Hong Kong Exchanges and Clearing Limited (HKEx) to meet future market development needs. It is built on an open, robust, secure and flexible modularised architecture with full fledged services that meets the business needs of market participants. It is designed to provide efficient and dynamic clearing and settlement by adhering to international standards for securities messages and providing interactive communication with market participants through a standard message-based application programming interface.

B. CCASS/3 Services

CCASS/3 provides (1) clearing and settlement services; (2) depository and nominee services; (3) security management services; and (4) collateral management services to the market intermediaries.

Clearing and Settlement Services

CCASS/3 is a book-entry system supports clearing and settlement of transactions traded in the Stock Exchange of Hong Kong Limited (SEHK). Trades will be settled on a continuous net basis or on a trade-for-trade basis. It also facilitates trade settlement among CCASS Participants via Settlement Instructions and Investor Settlement Instructions.

Stock settlement is electronically recorded as debits or credits to Participants' stock accounts in CCASS/3, without the physical movement of share certificates. While money settlement is effected with issuing of electronic debit and credit instructions against Participants' designated bank accounts.

Depository and Nominee Services

Physical share certificates deposited into CCASS Depository, which is the central depository operated by HKSCC, will become immobilised and transformed into electronic records in CCASS/3 to effect settlement.

Nominee services offered based on the electronic records distributes entitlements to participants and allows participants to take part in the corporate activities such as voting and subscription electronically via CCASS/3.

Collateral Management Services

The Common Collateral Management System (CCMS) provides an automated platform for flexible management of participants' collateral for securities or derivatives market products and in different currencies.

The system is equipped with a processing capability for a wider range of collateral types and collateralisation methods, which will include the entire process of valuating, calculating and administering the collateral that must be put up to cover open positions. Common collateral management service allows participants better use of assets to cover their financial commitments in different markets.

Apart from providing the services to the market intermediaries, HKSCC also allows investors to open Investor Accounts to participate as an Investor Participants in CCASS/3; or open Stock Segregated Accounts with Statement Service through their brokers or custodians.

Investor Account Services

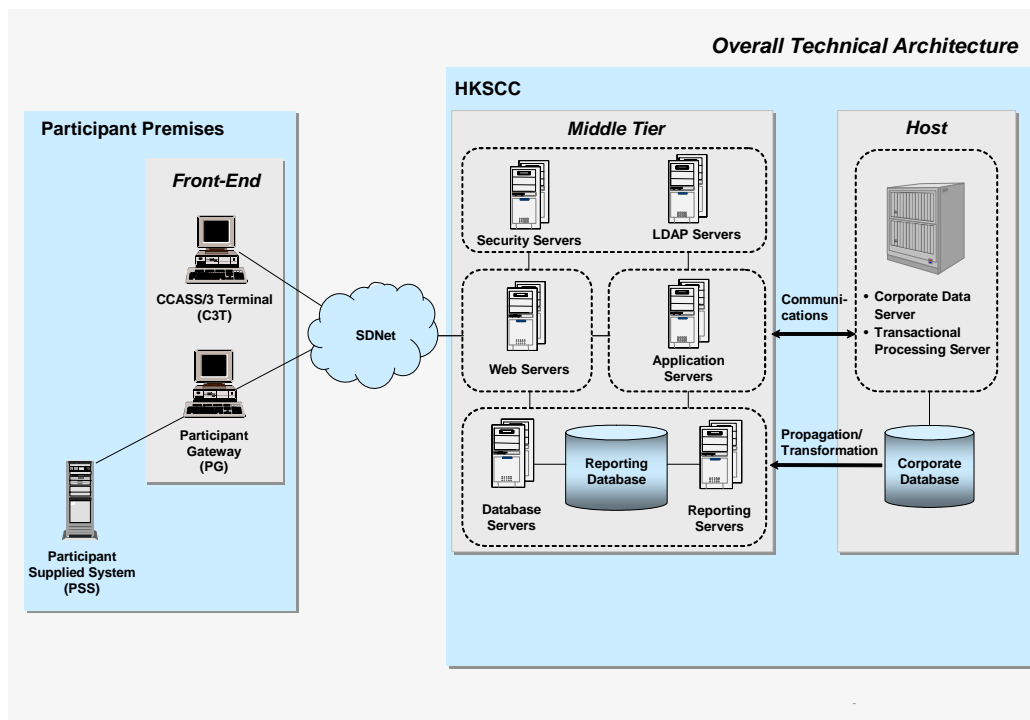
Investor Participants have legal title and physical control over their shares deposited in CCASS. Investor Participants can operate and manage their accounts via the CCASS Phone System or the CCASS Internet System.

Stock Segregated Account with Statement Services

Investors are able to check movements and balances of stocks in their Stock Segregated Accounts maintained in CCASS/3 under the name of their brokers/custodians. Furthermore, investors can give voting instructions and affirm stock transfers electronically through the CCASS Phone System and the CCASS Internet System.

C. CCASS/3 Technology Infrastructure

The efficiency and integrity of securities clearing and settlement depends on the functioning of the technology that underpins the infrastructure of the financial market. HKEx is committed to the use of the latest technology that forms the heart of the new clearing and settlement system.



CCASS/3 Host remains the database server for keeping the CCASS operation data to support batch processing.

The middle-tier between participant terminals and CCASS/3 Host supports access methods, such as web interface and Application Program Interface (API). Security servers and Lightweight Directory Access Protocol (LDAP) servers are employed to provide a centralised authentication and authorisation service for controlling participant access.

The Securities and Derivatives Network (SDNet) is a robust and high efficiency closed user group network based on Optical Ethernet technology. It adopts the TCP/IP protocols with high security protection by means of firewall and intrusion detection system.

Participants can access the CCASS/3 system through two channels:

- CCASS/3 Terminal
- Participant Gateway.

CCASS/3 Terminal

Participants can access CCASS/3 through a browser-based terminal, the CCASS/3 Terminal (C3T), which uses market standard Internet technology. Any PC running HKEx supported versions of Microsoft Windows and IE browser is able to access all CCASS functions. All participant functions will be provided with an HTML (windows) based presentation. This standard graphical user interface will provide a user-friendly interface and will reduce training needs for participants.

Participant Gateway

Participant Gateway (PG) is a technical device to provide an access point through which a Participant Supplied System (PSS) can access CCASS/3.

In order to reduce the development efforts of participants, Java-based application programming interfaces are provided to participants' PSS to communicate with CCASS/3 through the PG. The application program is a custom-built Java library that will assist the connection and handle all the subsequent message interactions between participants' back office system and CCASS/3 Host.

Hypertext Transfer Protocol Secure (HTTPS) is used for communication between PG and CCASS/3 middle tier. Socket is the communication method between PG and PSS. The message format follows the industrial standards ISO 15022.

Network Communication Layer

The SDNet will ensure the reliable transmission of input between the user device and the host. The network will control the transmission of all information within the CCASS/3 system and will help to achieve the shortest possible response time even at the highest data through-put rates, ensuring fast and efficient clearing and settlement services at all times.

Furthermore, the network connection is also designed to allow access to the FinNet currently operated by Securities and Futures Commission (SFC). The FinNet is a community network built to connect all financial institutions including securities, derivatives, banking, insurance and all other licensed financial entities in Hong Kong, to effect straight-through-processing and ultimately real-time financial transactions such as delivery versus payment.

Security Measures

Security is a primary concern in the system design of CCASS/3. The following security measures are employed in CCASS/3 to ensure confidentiality and security:

Pre-defined User Group Authority

All participant functions are grouped into a number of user groups. The availability of user groups for participants is pre-defined by the system. CCASS/3 allows the delegation of administrative privileges to organisational administrators, allowing them to manage user privileges and benefits within their organisations.

CCASS/3 Terminal Level

Access to the CCASS/3 Terminal is authenticated by a smartcard as the security token using digital certificate X.509 format.

Message Level

Encryption is implemented through standard browser functions, using 128-bit Secure Sockets Layer (SSL) key to prevent transactions from being exposed to eavesdropping, tampering or message forgery risks.

Participant Gateway Level

As with C3T and message level of security, access to PG is also authenticated by smartcard and all data exchange between the PG and CCASS/3 Host are encrypted using 128-bits SSL keys.

Network Level

Firewalls, routers and intrusion detection devices are used to protect the CCASS/3 network from unauthorised access through the public internet.