Technical Requirements

CCASS TERMINAL REQUIREMENTS

INTRODUCTION:

All participants can access CCASS host system through a browser-based terminal, the CCASS/3 Terminal (C3T), which will use market standard browser-based technology. All participant functions will be provided with an HTML (Windows™) based presentation. This will provide a user-friendly graphical interface and will reduce training needs for participants.

Participants are required to access CCASS host system by direct electronic linkage through a C3T or multiple C3Ts, to be installed at the participants' offices. Participants are responsible for obtaining their own C3Ts. They should apply for and arrange the installation of the required SDNet/2 data communication links from the accredited vendor(s). Participants are also responsible for all costs (for example, maintenance or otherwise) relating to their C3Ts, such as related peripherals (hub, cable) and PC software.

CCASS/3 TERMINAL SPECIFICATIONS:

Highlighted below are the recommended PC configurations for C3Ts. For the latest C3T configuration details, participants are advised to refer to the ***CCASS/3 Terminal Installation Procedures***, which is available at HKEX website.

Item	Descriptions
Minimum Hardware Configuration	For all supported Windows platforms – Personal Computer with 1GHz or faster x86 (32-bit) or x64 (64-bit) processor – Memory: 1GB (32-bit) or 2GB (64-bit) – Local Hard Disk: 16 GB (32-bit) or 20GB (64-bit) of free space – LAN interface: Fast Ethernet card or Gigabit Ethernet card X 1 – Communication port: 1 USB port for smartcard reader or 1 COM and 1 PS/2 port for COM port reader

<table>
<tr><th>Item</th><th>Descriptions</th></tr>
<tr><td>Software Configuration</td><td>
– Operating System:
▪ MS Windows 7 Professional 32-bit or 64-bit[1] (Chinese or English) version with Service Pack 1 (Win7 Pro SP1)
▪ MS Windows 8.1 Pro 64-bit[1] (Chinese or English) version (Win8.1 Pro)
▪ MS Windows 10 Pro 64-bit[1] (Chinese or English) version (Win10 Pro)

– Browser:
▪ Internet Explorer 11 (IE 11)

– Java Runtime Environment:
▪ JRE 8u111 (32-bit)

– Adobe Acrobat Reader (for viewing circulars, available in CCASS/3 Commissioning Website):
▪ Adobe Acrobat Reader 11 or above

Notes:
1. Only 32-bit JRE are supported for C3T on any supported 64-bit Windows platform

Since the above software are released at different times by vendors, the combinations of Operating System, Browser and Java Runtime Environment supported are illustrated in the below table:

<table>
<tr><th></th><th>Win7 Pro SP1
JRE 8u111</th><th>Win8.1 Pro
JRE 8u111</th><th>Win10 Pro
JRE 8u111</th></tr>
<tr><td>IE 11</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Legend:
<table>
<tr><td>✓</td><td>Supported</td></tr>
<tr><td>✖</td><td>Not supported</td></tr>
</table>
</td></tr>
<tr><td>Security Device</td><td>
– Smartcard Reader:
▪ GemPCUSB-SL (IDBridge CT40)(USB), GemPCUSB-SW (USB) and GemPC410 (com port)
▪ These readers can be used on all supported Windows version
</td></tr>
<tr><td>Network Device</td><td>
– Hub and Cable:
▪ Only required for dual SDNet/2 links or multi-C3T sharing one single SDNet/2 link
▪ One Fast Ethernet (100Mbps) Hub or Ethernet Switch with 10/100 or 100/1000 auto sense and it must support standard UTP connections (100BaseT or 1000BaseT)
▪ One Category 5 (for 100BaseT) or Category 5E/6/6A standard UTP (unshielded twisted-pair) cable for each C3T (to connect the C3T to the Hub or Switch)
</td></tr>
</table>

Item	Descriptions
C3 Terminal LAN Port or Network Device setting for connecting SDNet/2	– Fast Ethernet (100Mbps): ▪ Speed – Auto ▪ Duplex – Auto – Gigabit Ethernet (1000Mbps) ▪ Speed – Auto ▪ Duplex – Auto ***Note:*** *Participant should contact their SDNet/2 accredited vendor if they require network port setting different from the above.*

DATA COMMUNICATION NETWORK:

CCASS/3 runs on SDNet/2, which ensures the reliable transmission of input between the user device and host. It will also act as broadcaster, sending simultaneous transmissions of information to all participants. The network will control the transmission of all information within CCASS host 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 time.

Participants' choice of data line speed depends on their transaction volumes, expected response time, and the costs they prepared to pay. Participants can opt to use single network line to support multiple C3Ts. Participants can install network lines with specific line speed based on their operational needs. Below is the recommended bandwidth of network line to support a specific number of active C3Ts:

Number of Active C3T	Recommended Bandwidth
1 - 14	1Mbps
15 – 29	2Mbps

There are 2 options for participants to set up the SDNet/2 connection with CCASS/3

- Option 1: Single link
- Option 2: Dual link

Based on their operational needs, participants can set up the network line(s) using either one of the 2 options. The extra line in option 2 is set up for contingency purpose - in case the main line breaks down. For option 2, network traffic will be automatically routed to the secondary link.

The below diagrams show the communication network set up under the 2 options.

Remark: Hub / Switch is not required if only one single C3T is connected to the router.

EXHIBIT 7.1A Single Link

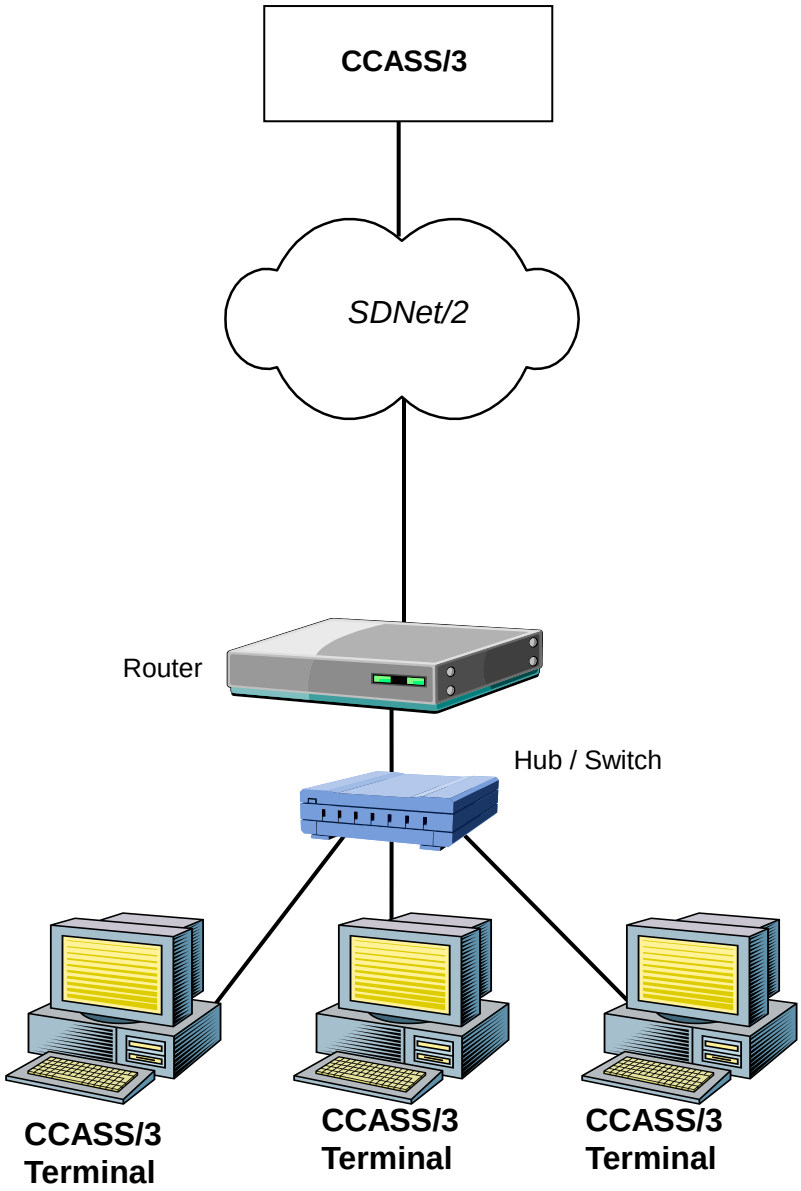
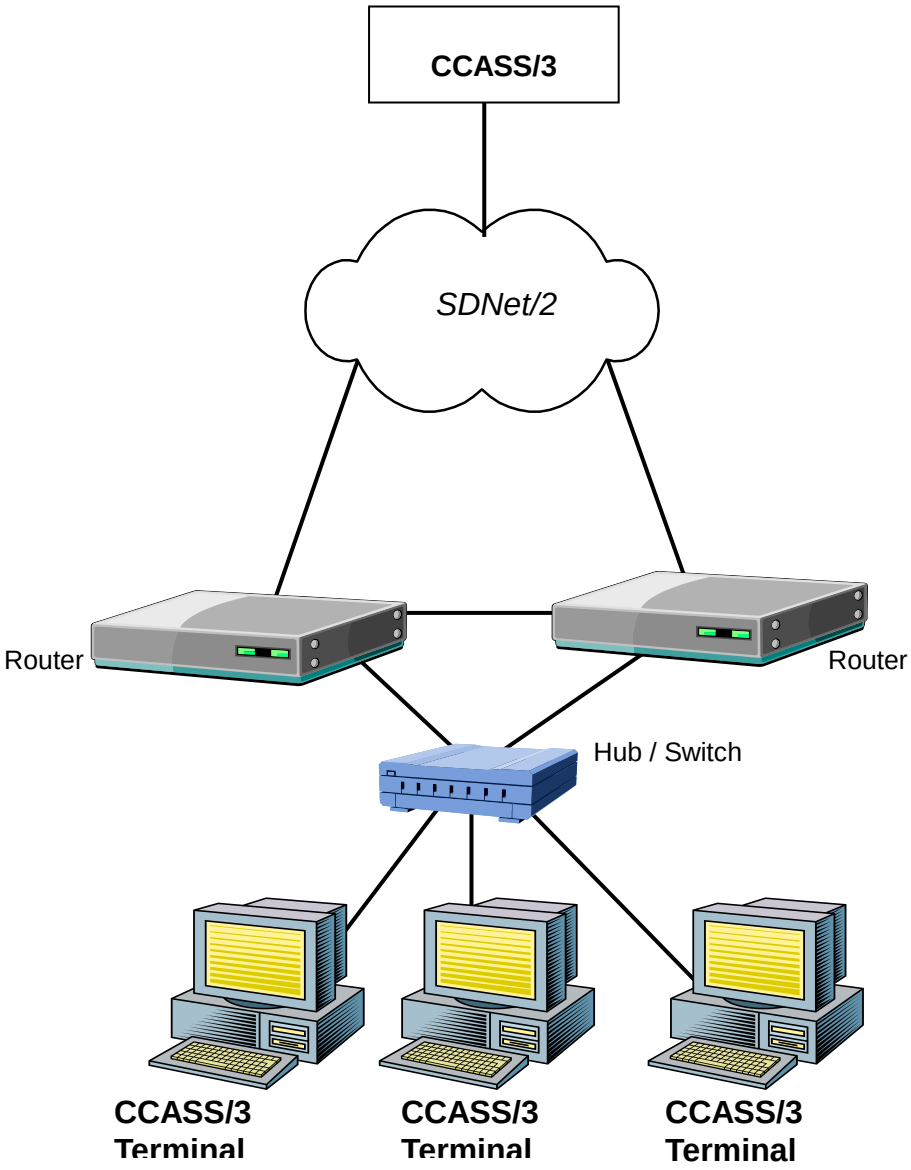


EXHIBIT 7.1B Dual Link



SMARTCARD AND SMARTCARD READER ("SC READER") :

Access to C3T is controlled by smartcard device. A SC Reader and a smartcard are required to be installed in the participant's C3T. Participants can purchase SC Readers and smartcards from HKSCC.

COMPUTER VIRUS / WORM SECURITY MEASURES :

Computer virus or worms are one of the concerns in security measure of computer system. Various security measures have been employed in CCASS design to protect it from computer virus or worms attacks. Participants are reminded that their C3Ts should be dedicated solely to accessing CCASS as uncontrolled access to the Internet will expose participants' C3Ts to various security attacks from the Internet. Besides, there are other potential sources of computer virus or worms e.g. use of external storage device with C3T for uploading or downloading CCASS information.

In view of the above, C3T users should pay attention and take proactive action to the security measures in their own C3Ts in the following two areas:

Virus protection

Participants are recommended to install anti-virus software on their C3Ts and regularly update the virus definitions from the vendor. For C3Ts not connected to the Internet, in some case, the vendor may make available the definition files daily in the Internet for download. Participants may download the updated virus definition file with a PC with Internet access, save the file in a disk or flash disk and install the update at C3T.

Microsoft OS patch

Participants are also advised to regularly review the latest Microsoft security patches and install them on their C3Ts accordingly. Participants may subscribe to Microsoft technical security notifications to keep up to date about security vulnerability and patches available: (http://technet.microsoft.com/en-us/security/dd252948.aspx)

For C3Ts not connected to the Internet, Microsoft security patches can be downloaded from Microsoft Download Center (or Microsoft Update Catalogue) separately with a PC with Internet access. Participants may then save the file in a disk or flash disk and install the patch at C3T.

Example Procedure:

1. Go to Microsoft Download Center: http://www.microsoft.com/downloads or Microsoft Update Catalogue: http://catalog.update.microsoft.com/
2. Search a particular security patch with the Security Bulletins Number (e.g. MS08-078) or Knowledge Base (KB) Articles number. (e.g. KB960714) that appears in the security notification.
3. Follow the instructions to download and save the file to disk or flash disk.
4. Use the disk or flash disk to install the patch on C3T. The patches may be in different formats, please follow Microsoft's instruction to install the patches.

PROHIBITED ACTIONS ON CCASS HOST SYSTEM :

Participants must not perform any unauthorised access or security scanning (no matter at network, system or application level) on the CCASS system and any related network device not owned by

them. Any such attempt will be regarded as illegal access or malicious intrusion to CCASS host system.