

Technical Requirements

CCASS TERMINAL REQUIREMENTS

INTRODUCTION:

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

Designated banks are required to access CCASS host system by direct electronic linkage through a C3T or multiple C3Ts, to be installed at the designated banks' offices. Designated banks 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). Designated banks 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 a 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 <ul style="list-style-type: none"><li data-bbox="587 1272 1098 1305">– Personal Computer with 1GHz or faster<li data-bbox="587 1305 794 1339">– Memory: 2GB<li data-bbox="587 1339 1066 1373">– Local Hard Disk: 20GB of free space<li data-bbox="587 1373 1369 1406">– LAN interface: Fast Ethernet card or Gigabit Ethernet card X 1 Communication port: 1 USB port for smartcard reader

Section 6.1

CCASS Terminal Requirements

Item	Descriptions
Software Configuration	<ul style="list-style-type: none"> - Operating System: <ul style="list-style-type: none"> o MS Windows 7¹ Professional 32-bit or 64-bit (Chinese or English) version with Service Pack 1 (Win7 Pro SP1) o MS Windows 8.1 Pro 64-bit (Chinese or English) version (Win8.1 Pro) o MS Windows 10 Pro 64-bit (Chinese or English) version (Win10 Pro) - Browser: <ul style="list-style-type: none"> o Internet Explorer 11 (IE 11) - Java Runtime Environment: <ul style="list-style-type: none"> o Oracle JRE 8u211² - CCASS Smartcard Client - Adobe Acrobat Reader (available in CCASS/3 Commissioning Website): <ul style="list-style-type: none"> o Adobe Acrobat Reader 11 or above <p>Notes:</p> <ol style="list-style-type: none"> 1. Microsoft announced support of Windows 7 is going to end on 14 January 2020. (https://www.microsoft.com/en-us/microsoft-365/windows/end-of-windows-7-support) Participants are required to upgrade to other support Operating System versions by Dec 2019. 2. One needs proper license subscription to download Oracle JRE 8u211. Please refer to details on (https://www.oracle.com/java/java-se-subscription.html) about Oracle Java SE Desktop subscription. And then download Oracle JRE 8u211 from (https://www.oracle.com/technetwork/java/javase/downloads/java-archive-javase8u211-later-5573849.html). Also please make sure CCASS Java Addon, if installed before, is uninstalled to use Oracle JRE 8u211.
Security Device	<ul style="list-style-type: none"> - Smartcard Reader: <ul style="list-style-type: none"> ▪ GemPCUSB-SL(IDBridge CT40)(USB) and GemPCUSB-SW (USB) These readers can be used on all supported Windows version
Network Device	<ul style="list-style-type: none"> - Hub and Cable: <ul style="list-style-type: none"> ▪ 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)

Section 6.1

CCASS Terminal Requirements

Item	Descriptions
C3T Terminal LAN Port or Network Device setting for connecting SDNet/2	<ul style="list-style-type: none">- Fast Ethernet (100Mbps):<ul style="list-style-type: none">▪ Speed – Auto▪ Duplex – Auto- Gigabit Ethernet (1000Mbps)<ul style="list-style-type: none">▪ Speed – Auto▪ Duplex – Auto <p>Note: <i>Participant should contact their SDNet/2 accredited vendor if they require network port settings different from the above.</i></p>

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 designated banks. 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 throughput rates, ensuring fast and efficient clearing and settlement services at all time.

Designated banks' choice of data line speed depends on their transaction volumes, expected response time, and the costs they prepared to pay. Designated banks can opt to use single network line to support multiple C3Ts. Designated banks 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 designated banks to set up the SDNet/2 connection with CCASS/3:

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

Based on their operational needs, designated banks 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.

Section 6.1
CCASS Terminal Requirements

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

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

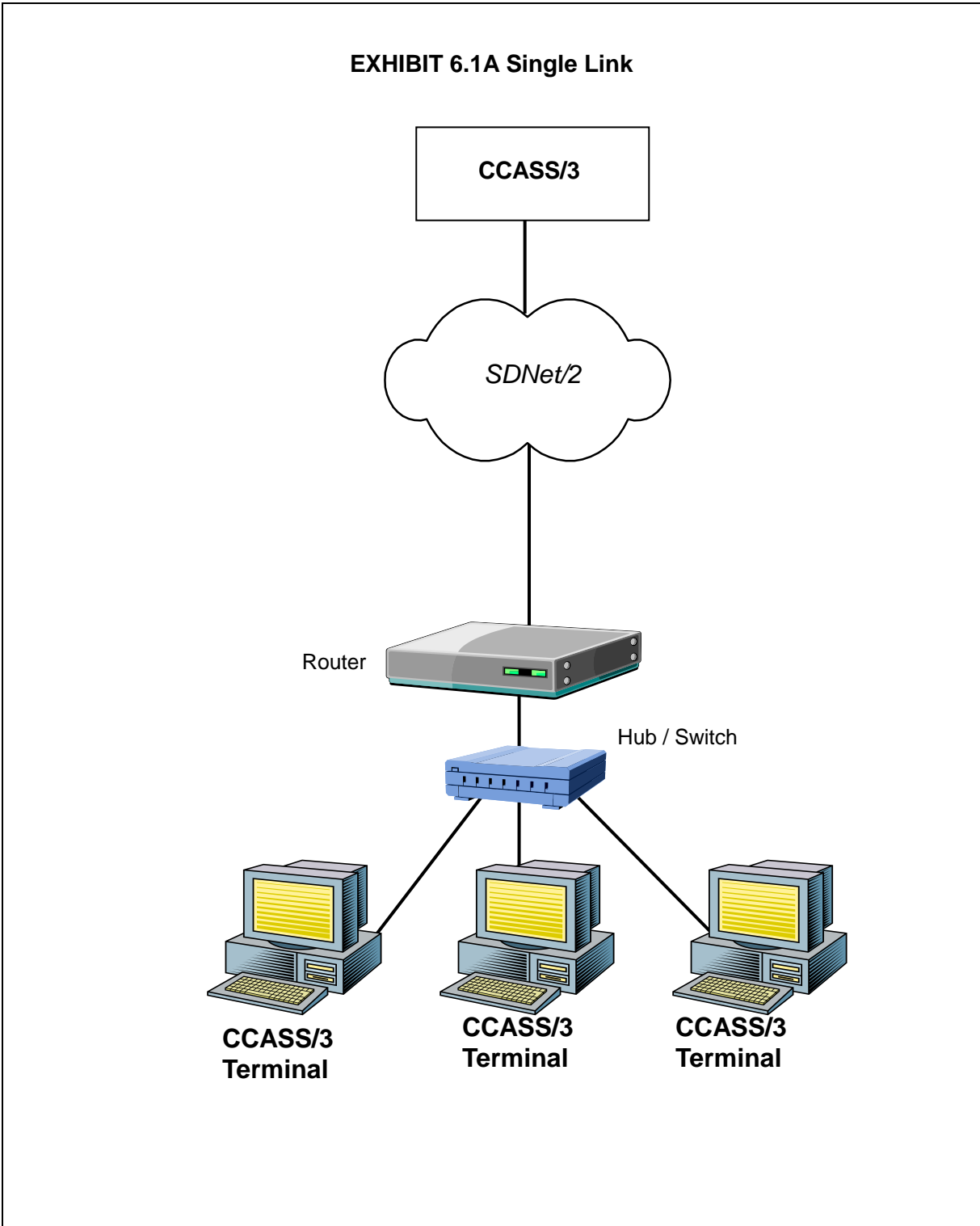
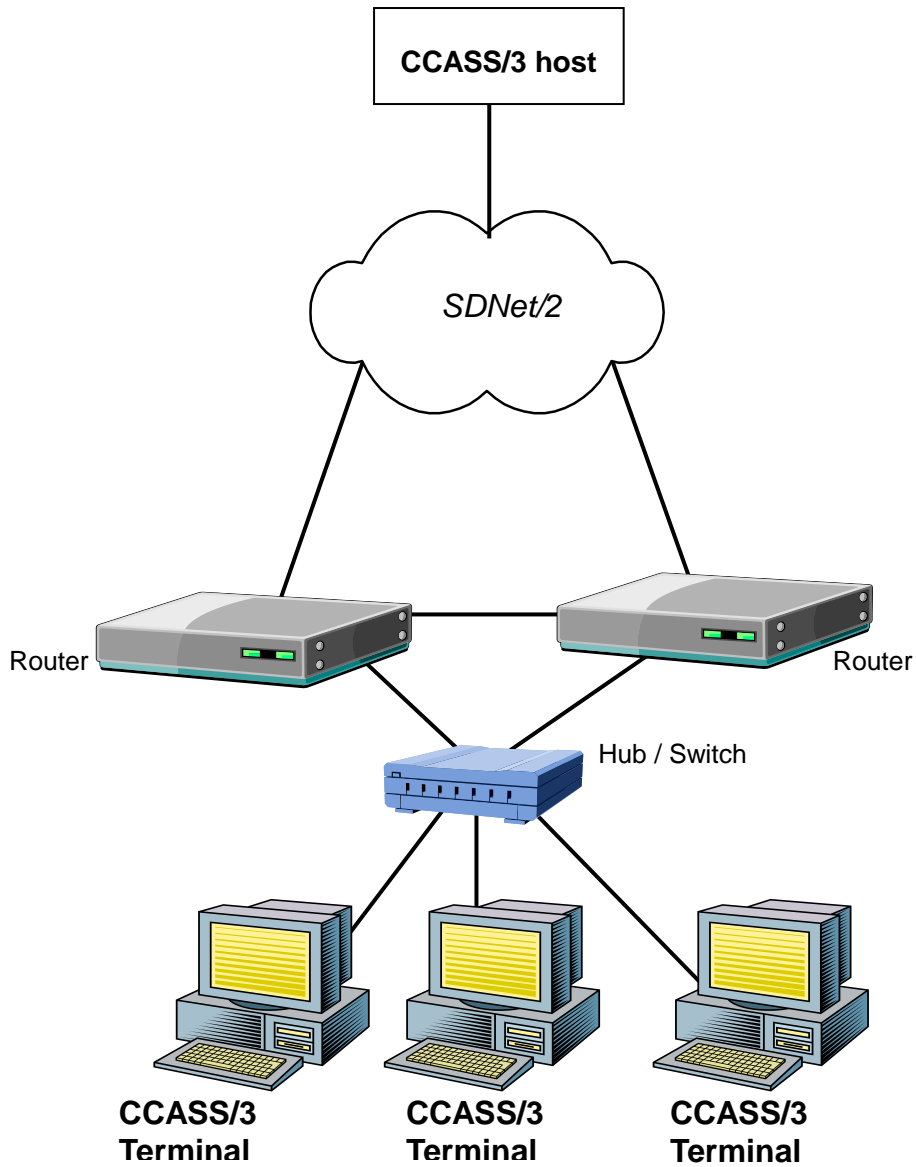


EXHIBIT 6.1B Dual Link



Section 6.1

CCASS Terminal Requirements

SMARTCARD AND SMARTCARD READER (“SC READER”) :

Access to C3T is controlled by a smartcard device. A SC Reader and a smartcard are required to be installed in the designated bank's C3T. Participants can purchase the Smartcards and SC Reader 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

Designated banks 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. Designated banks 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

Designated banks are also advised to regularly review the latest Microsoft security patches and install them on their C3Ts accordingly. Designated banks 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. Designated banks 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 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 system.