

System Configuration Requirements for eiMBT and eiCMT

1. Recommended System Configuration of eMBT and eCMT

eMBT and eCMT are certified to run on the following operating systems, browser versions as well as SWIFT components. Relevant technical supports may not be provided to members who adopt system configurations other than those listed below.

1.1 Operating System and browser

Microsoft Windows and Internet Explorer (IE) version:	(a) Windows 7 Professional SP1 – 32bit and IE11 (b) Windows 7 Professional SP1 – 64bit and IE11 (c) Windows 8.1 – 32bit and IE11 (d) Windows 8.1 – 64bit and IE11 (e) Windows 10 Enterprise – 64bit and IE11 (f) Windows 10 Professional – 64bit and IE11 Latest IE patch level is recommended.
---	---

1.2 SWIFT Related

WebAccess version:	(a) 7.0.40 (b) 7.0.50 (c) 7.0.55 (d) 7.2.54
JAVA version:	For WebAccess version 7.0.40/ 7.0.50/ 7.0.55 (a) Java 6 (Update 27 and up to Update 151) (b) Java 7 (Update 7 and up to Update 141) (c) Java 8 (Base and up to Update 131) Note: SWIFT only supports 32 bit versions of the JRE For WebAccess version 7.2.54 (d) Java 8 (Base and up to Update 181)
Digital certificate:	Digital certificate issued by SWIFT

Members should contact SWIFT at 2107 8777 for further details on the above software products to ensure that the relevant SWIFTNet connection and infrastructure, such as SWP, SAG, firewalls etc., are in place.

2. Recommended System Configuration of iCMT/iMBT

iCMT/iMBT is certified to run on the following operating systems and browser versions. Relevant technical supports will not be provided to members who adopt system configurations other than those listed below.

Microsoft Windows and Internet Explorer (IE) version:	(a) Windows 7 Professional SP1 – 32bit and IE11 (b) Windows 7 Professional SP1 – 64bit and IE11 (c) Windows 8.1 – 32bit and IE11 (d) Windows 8.1 – 64bit and IE11 (e) Windows 10 Enterprise – 64bit and IE11 (f) Windows 10 Professional – 64bit and IE11 Latest IE patch level is recommended.
Digital certificate:	Digital certificate issued by the following authorized issuers: (a) Local Certification Authority: (i) Digi-Sign Certification Services Limited (“Digi-Sign”) website: http://www.dg-sign.com ; (ii) Hongkong Post Website: http://www.hongkongpost.hk ; (b) Global Certification Authority: (i) Geotrust Website: http://www.geotrust.com ; (ii) VeriSign ¹ Website: http://www.verisign.com ; (iii) Symantec ² Website: http://www.symantec.com ; (iv) Entrust Website: http://www.entrust.com ; (v) IdenTrust Website: http://www.identrust.com ; (vi) DigiCert Website: http://www.digicert.com ; <small>¹ Security Business of VeriSign has been acquired by Symantec in 2010. ² Security Business of Symantec has been acquired by DigiCert in 2017.</small>

While HKICL has implemented multiple levels of security controls over internet access (including firewalls, application access authentication), internet connectivity may still have security implications on members’ networks and computers. As members can access the iCMT/iMBT through internet direct or any Internet Service Provider (ISP), they should ensure that the following basic security controls over access to the iCMT/iMBT via the internet are in place:

- Strong firewalls
- Virus protection software
- Anti-spyware software

- End-to-end encryption of data using SSL
- Comprehensive password policies

~~ END ~~