

CBEC Partners connectivity –Solution for agencies such as ICDs/CFSs not covered under the CBEC WAN/ LAN project & other agencies requiring connectivity with CBEC Datacenters – Version 2 (December 2010)

Reference: Reference is invited to CBEC Notification No. 26/2009-Customs(N.T.) dated 17th March 2009 bringing into effect the “Handling of Cargo in Customs Areas Regulations 2009” (referred in short as ‘Regulations’) and Circulars Nos. 13/2009-Customs dated 23rd March 2009 and No. 21/2009-Customs dated 4th August 2009.

The above Circulars issued by the CBEC prescribe that the networking, communication equipments, Uninterrupted Power Supply System, Computers/Personal Computers/Thin Clients, servers, printers and other computer peripherals as specified by the Directorate General of Systems shall also be provided by the custodians. It has further been provided that these instructions apply to all the Custodians of ports, airports, Inland Container Depots (ICDs), Container Freight Stations (CFSs) and Land Customs Stations (LCSs) except the major ports notified under the Major Ports Act 1963 and the airports notified under the Airports Authority of India Act, 1994.

Overview: This Document is meant to provide the technical details for connectivity of ICDs/CFSs not covered under CBEC WAN and/or LAN projects and other agencies requiring connectivity with CBEC Datacenters. This is part of the implementation process under CBEC’s IT Infrastructure Consolidation Project in which the following agencies are associated.

Responsible Agencies:

- a) Tata Consultancy Services – System Integrator for CBEC. TCS would also provide VPN clients as required after CBEC approvals.
- b) *TCL – Datacentre services provider for CBEC. Also one of the partner MPLS service provider.*
- c) *BSNL – WAN service provider for CBEC. Also one of the partner MPLS service provider.*
- d) National Informatics Centre - Application developer for ICES.
- e) DG (Systems), CBEC / PwC – Overall coordination and guidance.

Background: Container Freight Stations (CFS) are extended Customs examination areas for cargo and are attached to a Custom House. While Inland Container Depots (ICDs) have facilities for Customs documents filing and appraisalment in the case of CFS, document filing and appraisalment take place in the Custom House to which the CFS is attached.

In ICES Version 1.0, CFSs are connected to the local server in the Custom House by means of radio frequency (RF) wireless links or leased lines. Customs officers stationed in the CFS use these links to connect to the local ICES server to enter the examination reports for import and export cargo. Message interchange with the Custodians at the local Custom House level takes place through file transfer protocol (FTP) using a local message exchange server. With

Note: All changes from previous version are in italics

the move to ICES Version 1.5 on a centralized computing platform, the connectivity between the ICES 1.5 server and the CFSs need to be redesigned.

Infrastructure for Customs Officers in CFS / ICD without CBEC LAN/WAN

CBEC officers in CFS require the use of internet/MPLS to connect to ICES 1.5 servers at the CBEC Data centers. CBEC’s Primary Data Center (DC) is located at Delhi and the Disaster Recovery Site (DR) at Chennai. The internet solution envisages use of Virtual Private Network (VPN) solution over the Internet to secure the communication. VPN allows temporary creation or joining a private network (CBEC in this case) across an existing public network by creating an encrypted tunnel between two hosts. The tunnel enables transfer of information securely and to access remote resources.

Requirements:

- a) The Custodian would be required to provide MPLS / reliable Internet (minimum 2 mbps) connectivity to the Customs officers through a service provider of his choice. Both the options are explained in detail later in the document.
- b) The Custodian would be required to provide all the computing infrastructure including office space and furniture, desktops, LAN, File & print server, printers (including Line Printers as may be required), routers (if required), LAN Switches, air-conditioning, generator back-up and UPS. The annual maintenance for these equipment would also be his responsibility.
- c) Custodian is required to provide Linux based thin client to the customs officers posted in his CFS/ICD. Specifications for the thin Clients are given below. Details of the “Image” or software required for use with the thin clients may separately be obtained from Directorate of Systems & Data Management.

Thin Client Specifications	
Flash Memory	512 MB (Expandable upto 1 GB)
Main Memory	512 MB (Expandable upto 1 GB)
Processor	1 GHz
OS Support	Suse Linux 11.2

- d) Alternatively, Custodian can provide PCs with Pentium Core 2 Duo/1 GB RAM/ 40 GB HDD with Windows XP/ *Vista /Windows 7* and Internet Explorer and/or Mozilla Firefox browsers. CD drive / USB Drive (for storage functions) should be disabled. OS hardening /Password policy /Access control would be implemented in compliance with PC deployment policy *which would be forwarded separately. Please note that Windows 7 OS would work at sites connected by MPLS connection only as the VPN client for Windows 7 is not yet available.*

Note: All changes from previous version are in italics

- e) *Problems have been faced at various locations in using Line Printers with Windows PCs. Therefore CBEC does not recommend use of Windows PC directly with a Line Printer without use of a Linux based Print Server*
- f) PC's should be updated with latest antivirus Signatures. This is important since any violation would imply that the connectivity to the data center would be disallowed.
- g) *The custodians are advised to ascertain compatibility between all equipments and peripherals purchased as well as compatibility with CBEC setup depending on the connectivity options chosen. A list make/model of equipment already tried and found working and a compatibility matrix is placed at Annexure 1. It may however be noted that this list and the matrix is based on experience till date and may need revision based on further experience.***
- h) The Custodian would be required to have maintenance engineers for the IT equipment who would also act as the interface for technical issues. VPN Client software download and installation, configuration settings (including Username & Password), step By step Procedure for accessing the applications through VPN client will be provided by TCS after approvals from CBEC & the implementation will be carried out by the local maintenance engineers.
- i) The Custodian should ensure that the CBEC LAN is Insular and not connected to the CFS LAN. The CBEC LAN would also incorporate requirements, if any for service center. The Custodian will also ensure a separate connectivity to the Internet for CBEC.
- j) All custodians communicating with CBEC's Datacenters will be governed by CBEC's Information Security Policy. This would be provided separately by the Directorate of Systems.
- k) Custodians would be required to sign a "Non Disclosure Agreement" with the local Commissioner of Customs. The format of this agreement would be provided by the Directorate of Systems & Data Management.
- l) *Once the infrastructure is ready, the custodian is required to fill up the checklist enclosed at annexure 2, and have it verified by the Customs officer located at his site. The Customs Officer would in turn forward a scan copy of the signed checklist and NDA to PwC for issue of VPN id.(tripti.batra@in.pwc.com, subramanian.krishnan@in.pwc.com)*

Connectivity Options

Option 1 - Access through Internet:

In this option custodian can connect to the CBEC's datacenters through Internet by establishing secure connection to Datacenters. Each partner will arrange the Internet Connectivity (*minimum 2 mbps*) locally at their locations. For CBEC users for these locations,

Note: All changes from previous version are in italics

at Datacenter, Controlled access for the VPN users will be managed by TCS limited. *It is estimated that a 2 mbps connectivity would suffice for 5/6 concurrent nodes. However actual performance may differ depending on time, location and service provider.*

Option 2 - Access through the MPLS Cloud:

A custodian can connect with the MPLS Cloud of either BSNL or TCL. ***A bandwidth budget of about 100kbps per user can be used while deciding the bandwidth of the MPLS connection.*** *No VPN User & client software is required in case of MPLS connectivity.* CBEC has no objections to any other service provider being engaged by the partner subject to agreement between the service provider and TCL who are CBEC's data center providers. *CFSs that have already taken internet connection and need to switch over to MPLS may consider retaining the internet connection as back up link.*

Option 3 - Access through Point to Point Links:

In case of third option TCL/BSNL/any other service provider needs to build point to point links between various partner locations and the DC/DR of CBEC. In this case partner locations will be connected to DC/DR of CBEC on the separate Point to Point Links. These point to point Links will be terminated on Channel Partner Switch in the DC/DR. In view of the limited number of Ethernet ports, this option is being restricted to already identified message exchange partners only.

Note: This option is not available for private CFSs.

In all the available options listed above, CBEC will only work as a facilitator and the responsibility for arranging the actual connectivity remains with the partner agency. CBEC is only suggesting various options, which have different techno-commercial implications. The custodian may choose any option based on his business requirements.

Communication Mechanisms for Message Exchange

Following communication Mechanisms will be used for Message Transfer.

- (a) Secure file transfer protocol (SFTP)
- (b) Applicability Statement 2 (AS2)
- (c) Pretty Good Privacy(PGP)

Secure File Transfer protocol: With Secure file transfer Protocol, Users can pickup and drop files on the dedicated FTP server in the directories assigned to their respective user ids in a secure manner.

CBEC is considering Option (b) and Option (c) communication mechanisms and these will be used at a later stage when required.

Note: All changes from previous version are in italics