CBP Automated Manifest Interface Requirements

Requirements

May 2012

U.S. Customs and Border Protection

ace

Requirements

Communications provide trade community participants in the Automated Commercial Environment (ACE M1) the capability of transmitting data to and receiving data from the U.S. Customs and Border Protection (CBP) computer. CBP authorizes access to the ACE M1 for several categories of trade clients:

- Carriers
- Port Authorities
- Service Bureaus
- Rail
- Non Vessel Operating Common Carrier (NVOCC)
- Vendors
- Second Notify Party

The system is designed to use technology that is standard and readily available to both small and large businesses.

Several options are available to potential ACE M1 participants in the (CBP) Communications Interface Program. Software can be developed by the client or purchased from a vendor. Another possibility is to mailbox through a Value Added Network (VAN), or, if automation is a problem, securing the servicing facilities of a port authority or service center can be done.

The preparatory steps to become an ACE M1 participant are explained in this chapter, as well as the hardware and software requirements and testing procedures required for successfully completing the communications interface with ACE M1.

Respondent Checklist

A letter of intent or a completed Respondent Checklist found as an attachment to the list of Sea ACE M1 Data Processing Service Providers (available at www.cbp.gov and search for Sea Vendors) begins the process of becoming an ACE M1 participant. Please FAX your letter or Respondent Checklist to the following:

U.S. Customs and Border Protection
Client Representative Branch
7681 Boston Blvd.
ATTN: Beauregard, Room A-314-1
Springfield, VA 20598
FAX: (571) 468-5538

Upon receipt of the FAX, a Client Representative will be assigned to work with the interested party. The user must select a communications technique and protocol as well as undertake procurement of equipment and software.

The participant must provide an Interconnection Security Agreement (a.k.a. ISA). The link to the Instructions for Customs and Border Protection Interconnection Security Agreement (ISA) is:

www.cbp.gov/xp/cgov/trade/automated/automated_systems/isa/isa_instructions.xml

Communication Technique and Protocol

CBP provides five basic means of communications:

- Cisco VPN/MQ Series Solution via a client provisioned Internet Service Provider (ISP)
- Sprint or Verizon Multi-protocol Label Switching (MPLS) VPN (a private Cisco VPN/MQ Solution)
- Service Center
- VAN (value-added network)
- VPN via toll free dial-up where an ISP is not accessible

Potential participants decide which option best meets their business needs. To assist in this decision, a CBP Communications Specialist is available at the CBP Data Center at (800) 927-8729.

Procurement of Equipment and Software

Based on communications needs, the participant is responsible for ordering the necessary hardware and software. This information is best obtained through each participant's approved software vendor.

If the decision is to use the Sprint Frame Relay/MQ Series Solution, the participant must adhere to CBP's criteria by referencing the MQ Series/Frame Relay Enterprise Solution handbook that is accessible on www.cbp.gov or through a client representative office.

Pre-Test Requirements

When the trade participant completes equipment and software procurement, the trade participant must contact their assigned client representative and request a participant enrollment form. Once this form is complete, it is returned to the client representative who will facilitate the flow of the documentation to the proper personnel at the CBP data center.

Data center personnel will establish a ticket that will identify the request for a new network definition. This ticket will proceed as follows:

- Network Management Branch will establish and test IP connectivity
- Middleware Branch will establish queue names and test MQ channel connectivity
- Client Representative will verify data transmissions to the ACE M1 application

Once the ticket has completed this process and all phases of the ticket are successful, the ticket is closed.

CBP Pre-Test Responsibilities

Client Representative Branch personnel create the necessary client files in the CBP database in preparation for the communications interface test. These include files for the user, data processing site, and carrier. CBP's final pre-test responsibility is to verify the accuracy of information in the client files

Communications Testing

CBP data center personnel including the Network Management Team and Middleware Branch will work to resolve communications problems encountered during the initial interface attempt between the new client and the ACE M1 application. Once application testing commences, the client representative will facilitate any problems encountered.

Data Encryption Information

Encrypting the data to make it unrecognizable to most people will preserve the confidentiality of trade secrets, personal, financial, etc., data. The message text will become recognizable only after the automated decryption process has occurred.

The integrity of sensitive trade and Customs data will be preserved by the use of cryptography, automatic error detection and retransmission mechanisms.

The availability of the trade and CBP data will be preserved using automatic mechanisms such a alternate routing and network component redundancy.

CBP's three primary goals are to:

- Preserve the electronic data's confidentiality
- Integrity
- Availability