THE CUSTOMS & EXCISE DEPARTMENT

THE GOVERNMENT OF

THE HONG KONG SPECIAL ADMINISTRATIVE REGION

GUIDELINES FOR SETTING UP

THE SYSTEM-TO-SYSTEM INTERFACE

FOR EXCHANGING DATA WITH THE

ROAD CARGO SYSTEM (ROCARS)

[RT02]

Version 1.3

July 2019

AMENDMENT HISTORY

Amendment History				
Change Number	**Revision Description**	**Pages / Sections Affected**	**Revision / Version Number**	**Date**
1	Update of contact point information Supplement the digital certificate requirements for parties using the System-to-System Interface	Section 3.1 Section 3.5	1.1	February 2011
2	Update of contact point information	Section 3.1	1.2	April 2019
3	Update of contact point information	Section 3.1	1.3	July 2019

TABLES OF CONTENT

1.   INTRODUCTION

This document shows the major steps for the public users to connect their computer systems with the Road Cargo System (ROCARS) of the Customs & Excise Department (C&ED) via the system-to-system interface of ROCARS for exchanging data with ROCARS electronically.

The electronic data include both cargo information and bundling information in XML format. Public users should refer to the Implementation Instructions of the Road Cargo System (ROCARS) System-to-System Interface for Bulk Submission (ROCARS Technical Document Reference: RT01) for the detailed requirements of the XML messages structure and the message flow for implementing the computer application systems for exchanging data with ROCARS electronically.

Section 2 of this document highlights the standard configuration of the system-to-system interface. Section 3 and Section 4 highlights the steps for preparing and verifying the interface respectively.

Public users should follow the steps mentioned in Section 3 and Section 4 and to discuss with C&ED in detail to prepare and verify the system-to-system interface.

2. STANDARD CONFIGURATION

The system-to-system interface adopts Electronic Business using eXtensible Markup Language (ebXML) and ebXML Messaging Service (ebMS) as the messaging standards. It can be considered logically as a stack of 4 layers namely Application, ebXML, ebMS and Transportation. The diagram 1 below illustrates the relation of these layers.
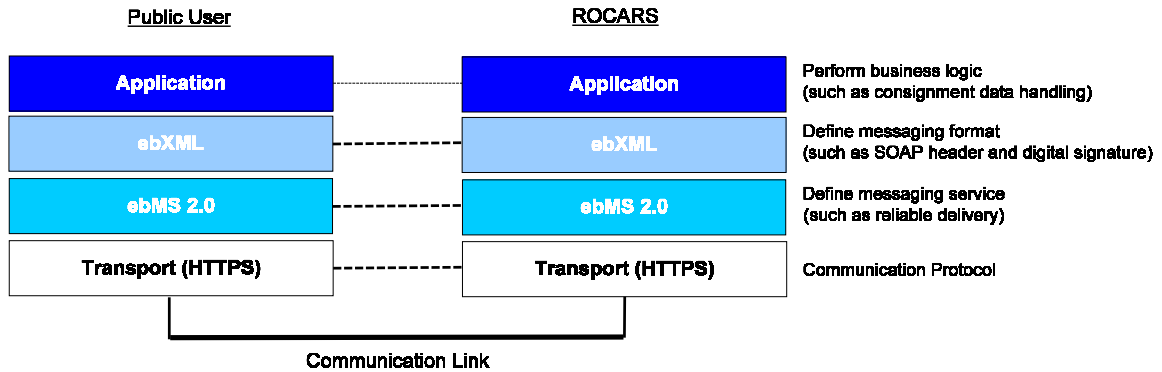
Diagram 1: Level of abstraction of the ebMS connection with ROCARS

A typical flow of the ebXML messages in the system-to-system interface is depicted in the diagram 2 below.

Diagram 2: ebXML message flow between a public user and ROCARS
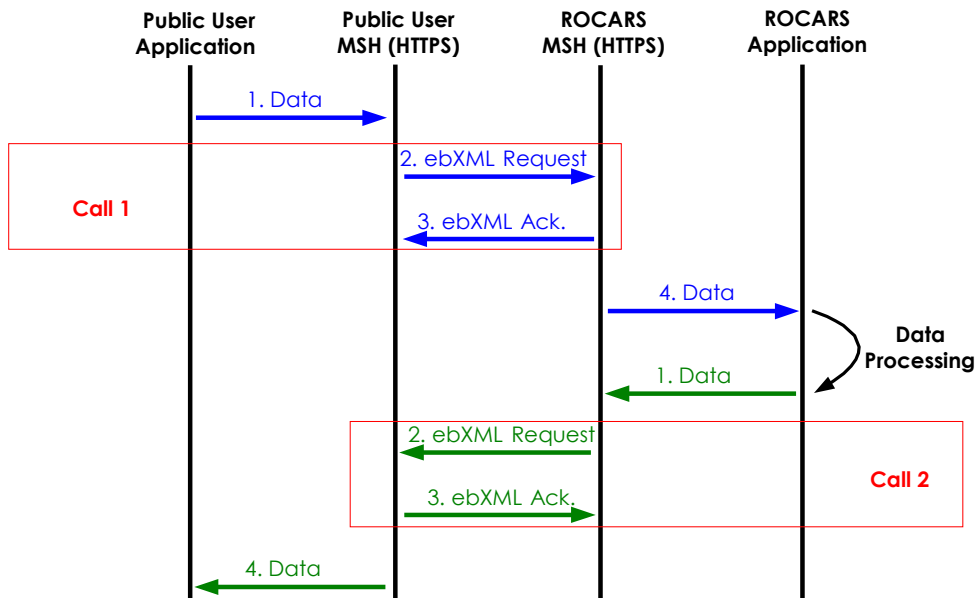
The computer systems of the public users can connect with ROCARS through the Internet or dedicated communication lines, i.e. Metro-Ethernet. The diagrams 3 and 4 below illustrate two examples of the structure of the network for the connection.
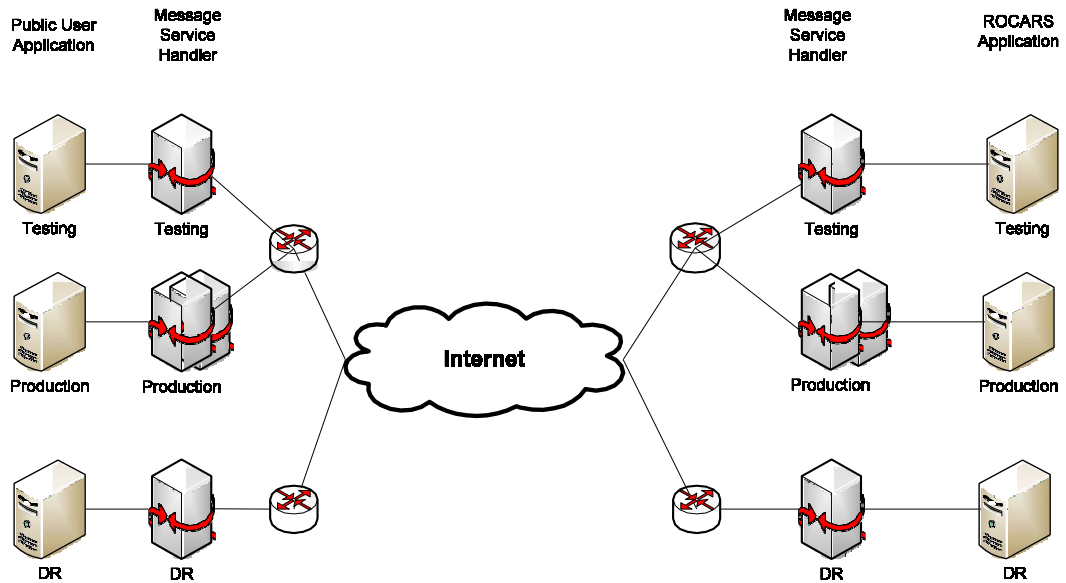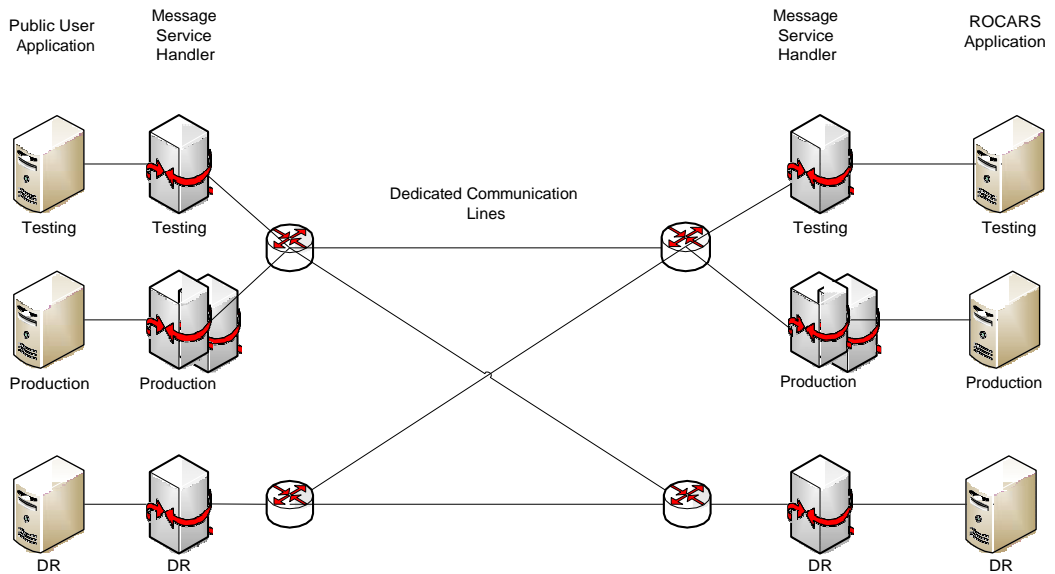

Diagram 3: Connecting with ROCARS via the Internet

Diagram 4: Connecting with ROCARS via dedicated communication lines

3. PREPARATION STEPS

The major steps for preparing the system-to-system interface are listed in sections 3.1 to 3.7 below.

3.1. Register with C&ED

- Contact C&ED to register the interest of connecting with ROCARS through the system-to-system interface for exchanging data with ROCARS.

  - On business and operation aspects –Ms. Alvina Ho
    e-mail : alvina_st_ho@customs.gov.hk   Telephone: 3152 0229

  - On technical aspects - Mr. Sam Chan
    e-mail : sam_ys_chan@customs.gov.hk   Telephone: 3759 2181

- After receiving the information, C&ED will further discuss with the user for the detailed arrangement and implementation plan.

- Register with C&ED as a ROCARS user.

3.2. Implement the Computer Application

- Implement the computer application system according to the Implementation Instructions of the Road Cargo System (ROCARS) System-to-System Interface for Bulk Submission.

3.3. Establish the ebMS Server

- Set up ebMS Message Service Handler (MSH) to act as the messaging gateway between ROCARS and the application system. It is recommended to set up three dedicated instances of MSH for production, testing and disaster recovery separately.

- Integrate the MSH with the application system to enable the application system to prepare and resolve the XML messages to and from ROCARS.

3.4. Establish the HTTP SSL Server

- Set up the HTTPS endpoints for the ebMS MSH(s).

3.5. Install a Digital Certificate for the Connection

- Acquire a digital certificate from a Hong Kong Recognized Certification Authority, i.e. Hong Kong Post or DigiSign, for signing the XML messages delivered to ROCARS.

- Associate the certificate with the corresponding ROCARS user account of the message signatory during ROCARS registration.

- Install the digital certificate into the ebMS server.

- Only 1 digital certificate of a user of a company registered in ROCARS can be treated as the valid message signatory of the System-to-System interface.

- The same digital certificate shall be used for signing the XML messages if there are more than 1 ebMS Message Service Handler (MSH) in a company.

- For change of the digital certificate of the user and change of message signatory of the System-to-System interface, please liaise with C&ED with prior notice of at least 7 working days before the change.

3.6. Establish the Network for the Connection

The systems of the users can be connected with ROCARS through the Internet or dedicated communication lines.

- Through The Internet
    - Acquire Internet connection for the user computer system.
    - Configure the Internet connection according to the specification provided by C&ED for communicating with ROCARS via the Internet.

- Through Dedicated Communication Lines
    - Acquire point-to-point dedicated communication lines to the ROCARS with the media and protocol agreed by C&ED.
    - Configure the communication lines according to the specification provided by C&ED.
    - The user shall be responsible for all the costs incurred for establishing the connection including that for Government ends of the communication lines.

3.7. Establish the Collaboration-Protocol Agreement (CPA)

- Provide the MSH end point address to C&ED. In return, C&ED will deliver the CPA(s) containing the end point addresses of both parties. It should be noted that if a user needs to use both the Internet and private network, he/she should provide two dedicated MSH end point addresses correspondingly for establishing two separate CPAs.

- Configure the MSH according to the CPA provided by C&ED.

- Configure the MSH to accept the ebXML messages delivered by ROCARS and verify the digital signature of the messages according to the ROCARS certificates (public key) provided by C&ED.

- ROCARS will associate the newly assigned ROCARS_PARTY_ID(s) with the corresponding ROCARS user account(s).

- At least two set of CPAs should be agreed between C&ED and the user, one for production and one for testing. Additional CPAs will be established with prior agreement and arrangement with C&ED for additional production and disaster recovery MSHs.

4. VERIFICATION STEPS

This section highlights the major steps for verifying the system-to-system interface.

4.1. Self Test

This section highlights the major test required for the user to conduct alone for the MSH. The user should conduct also the other normal tests required for computer system implementation such as unit test, function test, integration test etc.

4.1.1. Self Loop-back Test

- Simulate BOTH the user side and the ROCARS side ebMS parties based on the assigned CPA at the local MSH.

- Apply the following setting:
    - Both sides' endPoint URL should be pointed to the local MSH
    - Both parties should be configured to use the same certificate for both digital signature verification and signing
    - If self-signed HTTPS server certificate is in use for testing purpose, ensure the self-signed certificate chain is imported into the MSH's SSL trust store

- Deliver test messages between the two local ebMS parties until the messages are successfully sent and received at both sides.

- Finally, to get ready for connectivity test with C&ED, at the local MSH:
    - The ROCARS side endPoint URL should be changed to the value provided by C&ED
    - The verification certificate should be the ROCARS's certificate. That is, to grant ROCARS the authority to send message to this MSH

4.2. Joint Test

This section highlights the major tests for the MSH that require the effort of both the user and C&ED.

4.2.1. Connectivity Test

- Send the public key of the signing certificate to C&ED for ROCARS testing data preparation prior to the test.

- Send an ebXML message to the ROCARS testing server according to the testing CPA setting. The format of the testing message should follow the "Implementation Instructions of the ROCARS System-to-System Interface for Bulk Submission" document provided by C&ED.

- The ROCARS testing server will respond with an ebXML reply message digitally signed by the ROCARS testing certificate if the testing ebXML message is properly accepted and processed by the ROCARS testing server.

4.2.2. Application End-to-end Test

After all the ebMS level testing are completed successfully, an application level end-to-end test should be carried out.

The following business scenarios and messages are suggested to be tested with the details to be agreed between the user and C&ED:

Business scenario	Message Name	Function
Import Consignment	AIM	Fresh Submission
		Amendment
		Cancellation
Export Consignment	AEX	Fresh Submission
		Amendment
		Cancellation
Import Bundling	ACRID	Fresh Submission
		Amendment
		Cancellation
Export Bundling	ACRED	Fresh Submission
		Amendment
		Cancellation
Quick Bundling	QB	Fresh Submission
DI File Data Download	IDR	Download Request
	EDR	Download Request
All	All	Exceptional cases for the above scenarios and functions, if any

4.3.   Other Tests

Other tests such as test for the digital certificate and disaster recovery test will be carried out as and when required. C&ED will further discuss with the user to define the details of these tests in due course.

- END -