EUROPEAN COMMISSION
EUROPEAN ANTI-FRAUD OFFICE (OLAF)

Policy
Customs and Tobacco Anti-Fraud Policy; AFIS

Container Status Messages

Technical Implementation Guide for SFTP

Version 1.1

DOCUMENT HISTORY

Version	Date	Description
1.0	16/06/2016	Initial version
1.1	28/06/2016	Final version (after internal review)

INTRODUCTION

The amended Council Regulation EC 515/97 obliges carriers to transmit Container Status Messages (CSMs) for certain container movements with an EU-nexus, as of 1 September 2016. OLAF has established the supporting IT solution, referred to as the CSM directory. This document describes how to transmit these Container Status Messages to OLAF.

This document covers only the transfer of the messages. There is no specific Message Implementation Guide. OLAF will accept any X12 or EDIFACT messages which are standard-compliant, as stated in the Commission Implementing Regulation EU 2016/345.

CSM Compliance Guidance for Sea-Carriers can be found on OLAF website at the following address http://ec.europa.eu/anti-fraud/about-us/legal-framework_en

Environment

OLAF has implemented a dedicated server reachable through Internet via the SFTP protocol for CSM transmission purposes. Please note that CSMs transferred to OLAF are not accessible to other carriers.

The production environment is accessible as of 1st July 2016 with an availability of 24 hours/7 days to receive the Container Status Messages. Data transmitted before 1st September 2016 are deleted before go-live.

TRANSMISSION METHOD

An SFTP (aka Secure File Transfer Protocol) server has been setup by OLAF in order to receive the Container Status Messages (CSMs).

EDI MESSAGE TYPES

The carriers are requested to send CSMs using the EDI message types (ANSI X12 or UN/EDIFACT) currently used to exchange information with external parties (e.g. US Customs and Boarder Protection or industry partners). Carriers are requested to provide CSMs for the following events in so far as the data for these events is already generated and maintained in their IT system:

- Confirmation of booking;
- Arrival at a loading/unloading facility;
- Departure from a loading/unloading facility;
- Loading/unloading from a conveyance;
- Instruction of stuffing/stripping;
- Confirmation of stuffing/stripping;
- Intra-terminal movements;
- Terminal gate inspection.

FILE TYPES

Please provide the CSMs using ASCII encoded text files. Ensure that the filenames used for the transmitted files adheres to the following naming convention:

<carrier id>-YYYYMMDD-hhmmssSSS

Where:

<Carrier id>	The SCAC code (Standard Carrier Alpha Code) or the interchange sender identification currently used in the EDI message header (maximum 15 chars). This name should identify uniquely the carrier.
YYYYMMDD	The date of transmission
hhmmssSSS	The time of transmission including milliseconds, 24 hours time format, GMT time zone

Note: filenames must be unique

CONNECTION DETAILS

CSM SFTP server IP address: csm-sftp.olaf.europa.eu

CSM SFTP server authentication: username with SSH public/private key pair

HOW TO CONNECT TO OLAF

Upon initial connection the carrier is required to generate a SSH key (SSH2 RSA 2048 bits) and to provide the public SSH key to OLAF service desk (OLAF-CSM@ec.europa.eu). You will receive a confirmation from the OLAF service desk as soon as the registration of your public key is completed, together with the username you should use. As of this moment you should be able to upload data to OLAF CSM SFTP server.

Please send an e-mail to OLAF service desk OLAF-CSM@ec.europa.eu indicating when you have completed the upload of your first file. OLAF will verify the correct reception and provide you with a confirmation of receipt.

For SSH key instructions on how to generate SSH keys please consult Annex: SSH key generation instructions.

ACTING AS A BROKER

If you act as a broker and send CSMs on behalf of several carriers, the SCAC code should be specified inside every CSM. Your sender-id should also be specified in the EDI Interchange header of every CSMs.

A separate key-pair/username must also be used for each carrier.

TECHNICAL SUPPORT

For any technical issue occurring with the transmission of the files to the SFTP server, please contact the OLAF service desk: e-mail: OLAF-CSM@ec.europa.eu, Tel +32 2 296 27 27 (8h30-18h30 CET)

ANNEX: SSH KEY GENERATION INSTRUCTIONS

SSH KEY GENERATION ON LINUX / UNIX

Login to your host and issue the `ssh-keygen` command. You will be asked to provide the file to which you want to save the SSH key and the passphrase you want to use to protect the SSH key. An example of successful key generation is provided below.

```
# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_rsa.
Your public key has been saved in /home/user/.ssh/id_rsa.pub.
The key fingerprint is:
bb:8e:13:60:d4:08:c1:68:e2:91:5a:d7:f4:b9:04:5e user@machine.local
The key's randomart image is:
+--[ RSA 2048]----+
| o+o =o E        |
|o+o +.o+ .       |
|=..o  . +        |
|..  o  . .       |
|   . .  S        |
|      .  .       |
|       ..        |
|      .. .       |
|      .oo        |
+-----------------+
```

SSH KEY GENERATION ON WINDOWS

SSH keys can be generated using a wide variety of tools, the proposed utility in this procedure is the PuTTYgen utility which is part of the PuTTY package but can also be downloaded individually. Upon launching the PuTTYgen utility, a SSH key pair will be generated for you. You can leave the default settings in place: SSH2 RSA 2048 bits (**make sure it is selected**). Make sure you save the generated public and private keys before closing the utility.