Roadside Enforcement using a portable USB storage device

Revision 1.0

Table of Contents

1. Introduction

Continental has significant experience in designing and manufacturing of both secure on-board recording devices and dedicated, easy-to-use roadside enforcement solutions.

Any system designed to support the enforcement of restrictive legal requirements must be designed in such a way that law enforcement *always* has easy and immediate access to the data needed in order to perform the inspections. Any such system that does not fully support this basic requirement cannot be regarded as fit for purpose.

2. Summary

This document provides an overview of roadside enforcement scenarios based on the usage of a USB portable storage medium or USB Flash Drive (hereafter UFD). It also introduces examples of dedicated EOBR enforcement equipment that would increase performance and reduce cost.

The usage of a UFD based solution provides enforcement with a highly cost-effective, reliable solution for having instant access to electronic RODS files at the roadside, regardless of wireless network availability.

The UFD based approach can significantly reduce the time needed for the average roadside inspection, thereby increasing the number of inspections that could be carried out.

Such a system also promotes the separation of the core EOBR functionality, represented by the accurate recording, storage and delivery to enforcement of HOS records, from the requirements of fleet management systems. Telematics are primarily advantageous in the fleet management paradigm and should not be assumed to be a fundamental part of an EOBR. The market will ensure that telematic capability is leveraged between the EOBR and host systems for carriers that require such features. For enforcement, the telematic approach brings no advantages, but it does incur significant cost and very high complexity (see *Framework for Telematics Application Services Approach—DRAFT.docx* for details).

3. Security of USB based enforcement Systems

3.1 Data Integrity Protection

The FMCSA document *"DRAFT_EOBR_Security_Requirements.pptx"* provides the security requirements for EOBRs. This document includes the following clear requirements:

- ***Data at rest must be protected***
- ***Data in Transit must be protected***
- ***The EOBR shall protect EOBR data collected, stored, disseminated, or transmitted from inadvertent alteration, spoofing, tampering, and other deliberate corruption***

Non-PII data can be protected highly effectively using the concept presented in Continental's document *"EOBR_Security_Concept_Proposal_v1.0"*. Furthermore, a simple extension of this concept could provide for the encryption of PII data. Usage of this concept provides the needed data protection for both telematic and peer to peer, e.g. UFD, based enforcement systems.

In order to fulfill key security goals such as non-repudiation, and data authenticity, Continental recommends adoption of such a PKI based data integrity protection concept.

3.2 Response to Qualcomm's Risk Analysis

In the document *Risk Analysis of USB Data Communication for EOBRs*, Qualcomm presented their view of security concerns regarding the usage of wired USB storage devices. Continental does not concur with this view, but supports the detailed and objective analysis provided by Zonar in *Evaluation of Qualcomm's* "Risk Analysis of USB Communication for EOBRs Rev. 1.4"[1].

In addition to Zonar's comments, we would add the following statements.

3.2.1 Authentication

> *Qualcomm:*
> *"Lack of Secure Authentication. USB connection between two devices provides no way of verifying identities of either device."*

In a telematic data transfer, where the two sides of the data exchange are not visible to one another, strict authentication is required. However, in the roadside scenario where the driver can see the enforcement officer and the enforcement officer can see the driver and the certified EOBR, such authentication is not necessary.

As Zonar pointed out "*the officer would be able to observe this operation*". In the same way that an enforcement officer could recognize a certified EOBR with red/yellow/green screens, he/she can identify that the UFD is inserted into the certified EOBR.

Strong authentication of the EOBR itself can also be provided as discussed in Section 3.1Data Integrity Protection.

3.2.2 Malware & Authorization

> *Qualcomm:*
> *"Unauthorized Read/Write/Code Execution. The most common ways of connecting devices via a USB connection do not provide sufficient protection against unauthorized data access on EOBR devices and requires additional security measures"*

[1] With the exception that Continental does not agree that a centrally FMCSA managed system for RODS retrieval is either preferable or cost effective.

> *"Malware. USB Malware is a highly likely attack vector which can infect or disable a large fraction of both EOBR devices and law enforcement computers"*

Continental regards these concerns as unfounded. In the future, the EOBRs will be independently certified, and even most of today's AOBRDs are fitted with USB connectors and manufacturers must protect their products against being compromised by any USB device that is inserted.

The UFD itself would be provided by enforcement and as such would not be malicious. Nonetheless, during a roadside inspection the certified EOBR would not read from the UFD, but would only write RODS files hence rendering the transaction completely harmless.

For those states that do not allow USB devices to be inserted into enforcement computers, alternative solutions are proposed in Section 4.

3.2.3 USB Physical Limitations

> *Qualcomm:*
> *"Physical Limitations of USB Connections. USB 2.0 standard specifies the maximal* 26 *length of a USB cable to be 16.4 ft (5 meters), which might be insufficient for most* 27 *intended uses of a USB connection with EOBR devices"*

Continental would not recommend a wired solution due to the impracticality of using such a long cable during a roadside inspection. Use of a UFD therefore removes this concern.

4. Roadside Scenarios

There are three principle roadside scenarios:

- enforcement equipment (laptop) is available that is permitted to use a UFD
- enforcement equipment (laptop) is available that is not permitted to use a UFD
- enforcement equipment (laptop) is not available

For all three scenarios, a significant time saving can be realised by using an Intelligent Inspection UFD as described in Section 5.1.

It should be noted that in all the scenarios described, no exchange of information between the driver and the enforcement officer e.g. PINs is needed.

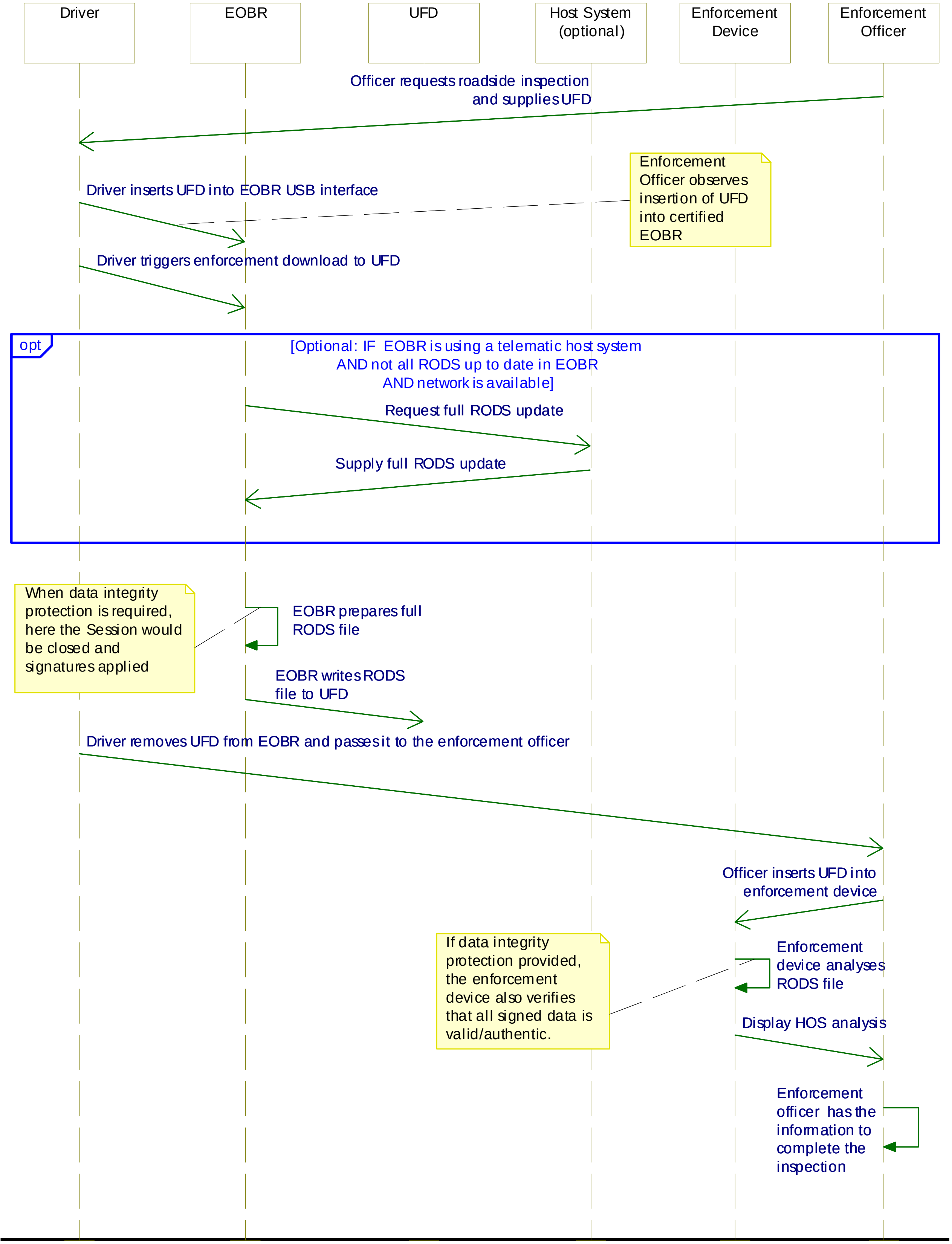
4.1 Enforcement Equipment (laptop) permitted to use UFD

This scenario is the normal case in which enforcement equipment may be used with UFDs.

The sequence diagram below also shows the optional connection of the EOBR (not enforcement device) to a host system via telematics in order to ensure all the RODS data is present on the EOBR before storing to the UFD. For the sake of simplicity, the diagram does not show the various possible error cases e.g. if no network connectivity is available for the EOBR.

The key elements of this scenario are:

- The UFD is supplied by the enforcement officer.
- The driver must trigger the enforcement process that results in storing the RODS data on the UFD.
- The enforcement officer can observe that the UFD is inserted into the certified EOBR.
- The required data needs to be present on the EOBR.
- Enforcement equipment (laptop) is available to analyze the RODS file.


Driver
EOBR
UFD
Host System (optional)
Enforcement Device
Enforcement Officer
Officer requests roadside inspection and supplies UFD
Enforcement Officer observes insertion of UFD into certified EOBR
Driver inserts UFD into EOBR USB interface
Driver triggers enforcement download to UFD
opt
[Optional: IF EOBR is using a telematic host system AND not all RODS up to date in EOBR AND network is available]
Request full RODS update
Supply full RODS update
When data integrity protection is required, here the Session would be closed and signatures applied
EOBR prepares full RODS file
EOBR writes RODS file to UFD
Driver removes UFD from EOBR and passes it to the enforcement officer
Officer inserts UFD into enforcement device
If data integrity protection provided, the enforcement device also verifies that all signed data is valid/authentic.
Enforcement device analyses RODS file
Display HOS analysis
Enforcement officer has the information to complete the inspection

4.2 Enforcement Equipment (laptop) not permitted to use UFD

The flow of this scenario is essentially identical to the flow above, just the UFD would not be inserted directly into the enforcement device (laptop), but into a simple dedicated device that would transfer the data from the UFD to the enforcement device (laptop) via a permitted interface e.g. WLAN, Bluetooth, serial connection, etc.

4.3 Enforcement Equipment (laptop) not available

This very common scenario can be solved by inserting the UFD into a dedicated mobile enforcement device. Such a device is described briefly in Section 5.2 Roadside HOS Analyzer.

Due to the affordable nature of such a device, and the lack of infrastructure needed to implement and maintain it, this scenario can provide an effective method to quickly equip large numbers of enforcement officers to perform effective roadside inspections on trucks fitted with EOBRs.

5. Supporting Equipment for roadside inspections

This section contains examples of two pieces of equipment that could be used to perform roadside inspections. The use of such equipment

- ***could significantly decrease the time spent for an inspection,*** and hence
- ***could increase the number of inspections that can be conducted in a period of time***.

5.1 Intelligent Inspection UFD

Instead of just a simple mass storage UFD, a low-cost intelligent UFD could be used. Such a device would be inserted into the EOBR as in the above scenario and would behave as a mass storage UFD. However, the device would also have the intelligence to check the integrity of the RODS data (provided data integrity mechanisms have been implemented in the EOBR concept) and to perform the HOS calculation.

Via LEDs on the device the enforcement officer gets instant feedback regarding any HOS infringements in the data. For example red, yellow, green. As this analysis is performed by an enforcement device, the level of trust for the enforcement officer will be significantly higher than observing a colored screen in the cab. When combined with data integrity protection, this approach is highly trustworthy.

If the intelligent inspection UFD indicates that an infringement has occurred, the officer can transfer the data on the UFD onto enforcement equipment (laptop) in the vehicle. Such an intelligent UFD could easily be provided with a second interface to connect to enforcement hardware that would also be acceptable to agencies that do not permit USB connections e.g. WLAN, RS232, Bluetooth, etc.

For the cases where such enforcement equipment (e.g. a laptop) for performing the full HOS analysis is not available in the enforcement vehicle, a dedicated device can be used. See 5.2 Roadside HOS Analyzer.

If the intelligent inspection UFD indicates that no infringement has occurred, both the driver and the enforcement officer can move on with an absolute minimum of time having been spent. Usage of such an enforcement device genuinely leverage the advantages of an Electronic On-Board Recorder.

Possible example of an Intelligent Inspection UFD

5.2 Roadside HOS Analyzer

The picture below represents a possible example of a dedicated roadside HOS analyzer. Enforcement officers could be equipped with such devices, especially where no other equipment such as a laptop is available.

A simple mass storage UFD or an intelligent inspection UFD can be inserted into the USB interface of the roadside HOS analyzer and the integrity check plus full HOS analysis performed, with on-screen results and the possibility to show a graphical representation or to drill down into the data as needed.

The roadside HOS analyzer would also be fitted with further interfaces allowing acceptable methods of connection to back-office enforcement systems for further processing and archiving of data.

As such a device would be custom designed and built for mobile use it would be robust and, unlike many PC based systems, would have a very high level of availability.

Possible example of a mobile Roadside HOS Analyzer