Approach for Secure Peer to Peer Roadside Log Downloads for EOBRs

Revision 1.3

1. Introduction

Continental has significant experience in building secure on-board recording devices, including the provision of data download/transport mechanisms and back office solutions for fleet management as well as cost-effective equipment for law enforcement purposes.

This document proposes a secure peer to peer EOBR roadside log downloadusing Bluetooth technology.

2. Summary

This document demonstrates that a secure peer to peer, offline, enforcement process can be provided at very low cost to both the fleets, indivual drivers and enforcement agencies. This can be achieved with existing, off-the shelf, technology and minimal infrastructure.

It avoids all the cost, complexity, fallibility and security risks of a highly distributed telematic system and it provides maximum availability for drivers and enforcement agencies.

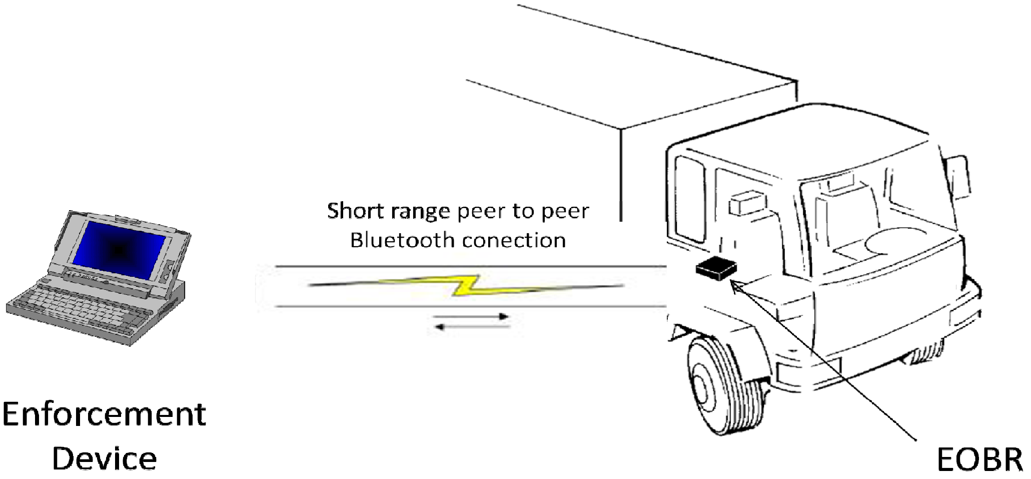
Bluetooth has been chosen in preference to a wireless 802.11 solution as Bluetooth:

- was essentially developed for such peer to peer usage scenarios in contrast to 802.11 which is designed as a networking standard
- is simpler to configure
- is significantly lower cost.

Due to the improved pairing security, the use ofBluetooth 2.1 is recommended.

3. Conceptual Framework

3.1 Overall architecture



The figure shows a comparatively simple architecture. No additional infrastructure for the enforcement is needed. The driver log file is transferred directly, using Bluetooth (BT) technology, to the enforcement device after a successful authentication procedure.

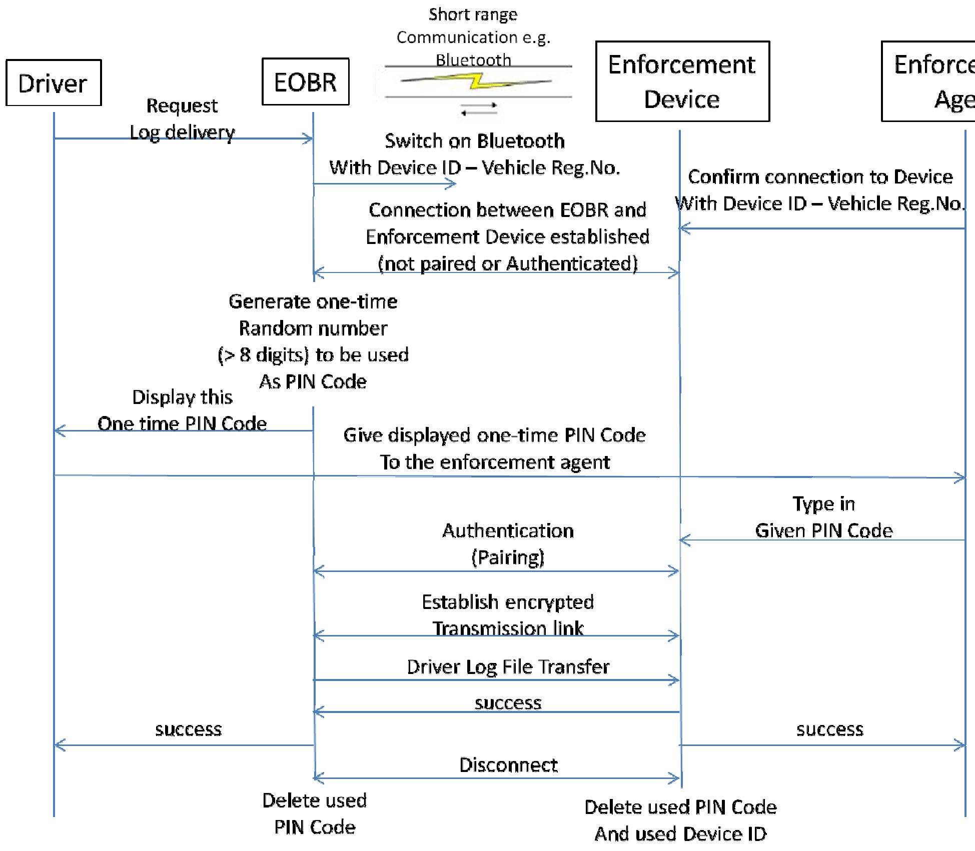
3.2 Detailed process

The initial steps were performed within normal usage of EOBR. The driver authenticates himself at the EOBR with his driver identification (ID, password or equivalent identifier). The request for an electronic log data roadside inspection is a face to face interaction between the enforcement agent and the driver.

There are several possibilities to provide low-cost secure communication between the enforcement device and the EOBR. Here is a non-exhaustive list of such scenarios, followed by a more detailed description:

- Internal BT connectivity with authentication key generated by the EOBR.
- Internal BT connectivity with authentication key generated by the enforcement device.
- Internal BT connectivity with device name and authentication key generated by the EOBR.
- Internal BT connectivity with device name and authentication key generated by the enforcement device.
- BT connectivity using pre-paired enforcement dongles.

3.2.1 Internal BT connectivity with authentication key generated by the EOBR

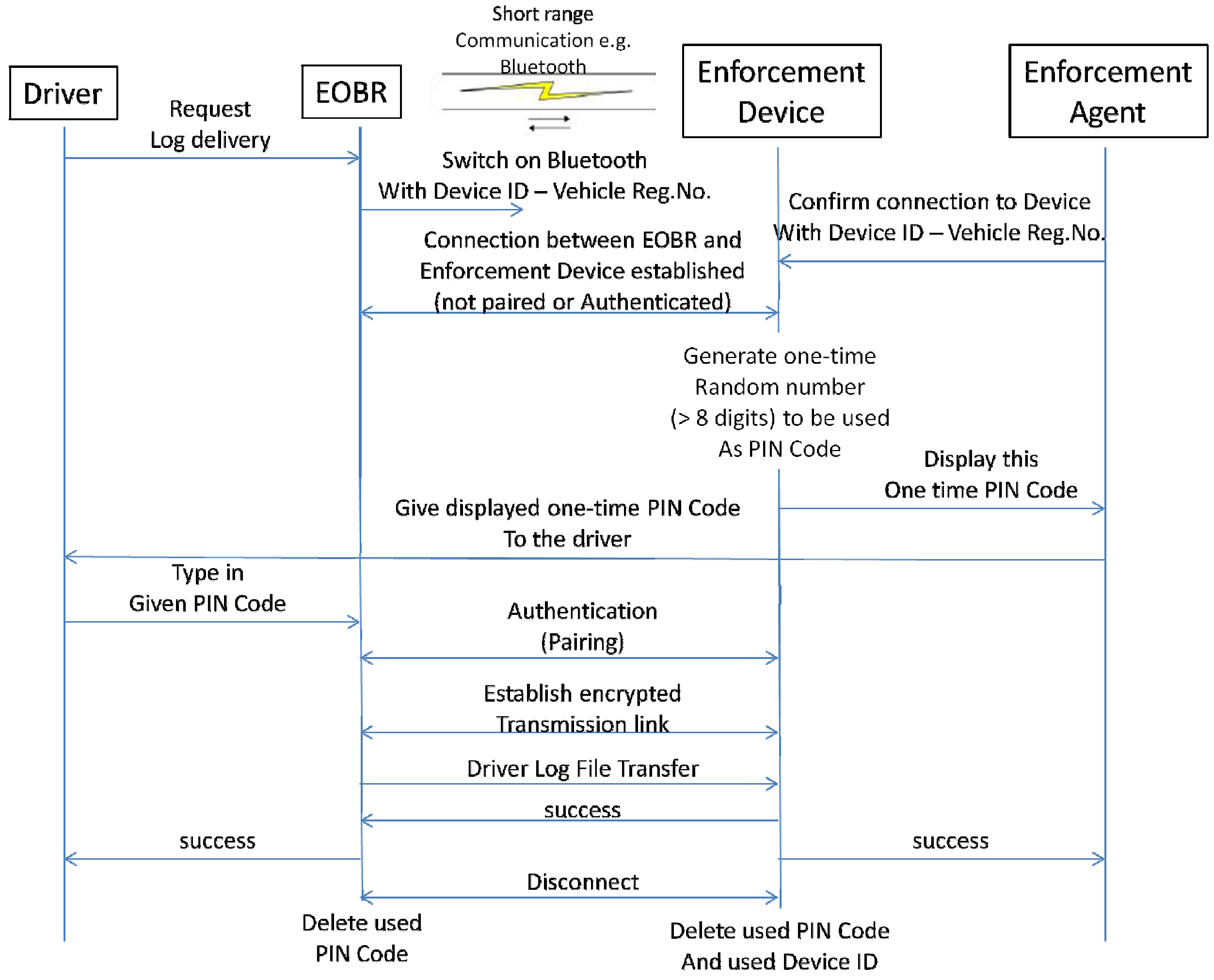


1. The enforcement agent requests an RODS file from the driver, who uses the EOBR to start the log delivery process. The EOBR starts to transmit its device name– in this case that could be the vehicle registration number as calibrated during the EOBR istallation. If this is not unique, any combination of data that is identifiable by the enforcement agent could be used, e.g. vehicle registration number plus driver name or vehicle registration number plus EOBR device ID.
2. The enforcement agent, using almost any bluetooth capable device e.g. PDA, SmartPhone, Laptop/PC, can scan for available BT devices, and select the correct one. There may be several devices available, the device name described ensures that the correct device is selected. In the event of a spoofing attack by a fake EOBR, the connection would be established, but the authentication described below would fail.
3. The two devices negotiate a stable physical connection, and enter the “connected” mode. At this point no authentication has taken place and data exchange is not yet possible.
4. The EOBR generates a random number (the PIN), which should be longer than 8 digits.
5. This PIN can be shown on the display of the EOBR and/or printed out via the integrated printer. The printout could contain just plain text or machine readable versions of the PIN e.g. bar code or QR code. The code can also be verbally given to the enforcement agent by the driver.

The enforcement officer can directly observe that the driver is reading from, or has provided the printout from, the EOBR being controlled.

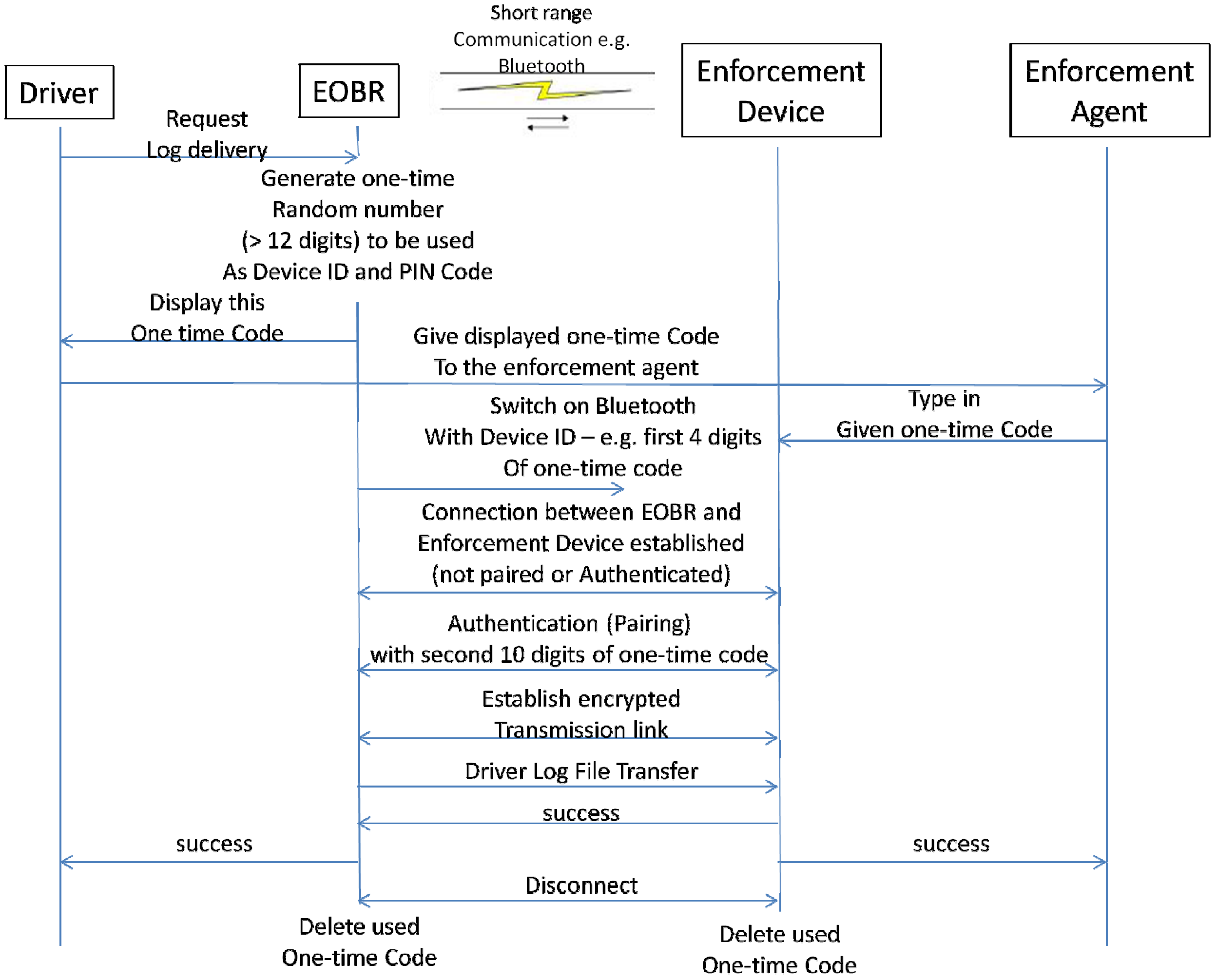
6. The enforcement agent enters the PIN into the enforcement device. This PIN is only known to the two participants in the communication, not to a possible attacker. Based on this PIN,the two devices will perform the pairing operation and negotiate encryption keys. Now the communication is encrypted and secure, with the correct EOBR.
7. The RODS file is transferred from the EOBR to the enforcement device
8. If necessary the correct reception can be confirmed
9. The connection is then closed and the pairing information, including the PIN is deleted.

3.2.2 Internal BT connectivity with authentication key generated by the enforcement device



1. Same as 3.2.1.
2. Same as 3.2.1.
3. Same as 3.2.1.
4. The enforcement device generates a random number (the PIN), which should be longer than 8 digits.
5. This PIN can be shown on the display of the enforcement device. The PIN can be verbally given to the driver, or shown to the driver on the display of a mobile enforcement device.
6. The driver enters the PIN into the EOBR. The enforcement officer can directly observe that the driver enters the PIN into the EOBR being controlled. This PIN is only known to the two participants in the communication, not to a possible attacker. Based on this PIN, the two devices will perform the pairing operation and negotiate encryption keys. Now the communication is encrypted and secure, with the correct EOBR.
7. Same as 3.2.1
8. Same as 3.2.1
9. Same as 3.2.1

3.2.3 Internal BT connectivity with device name and authentication key generated by the EOBR

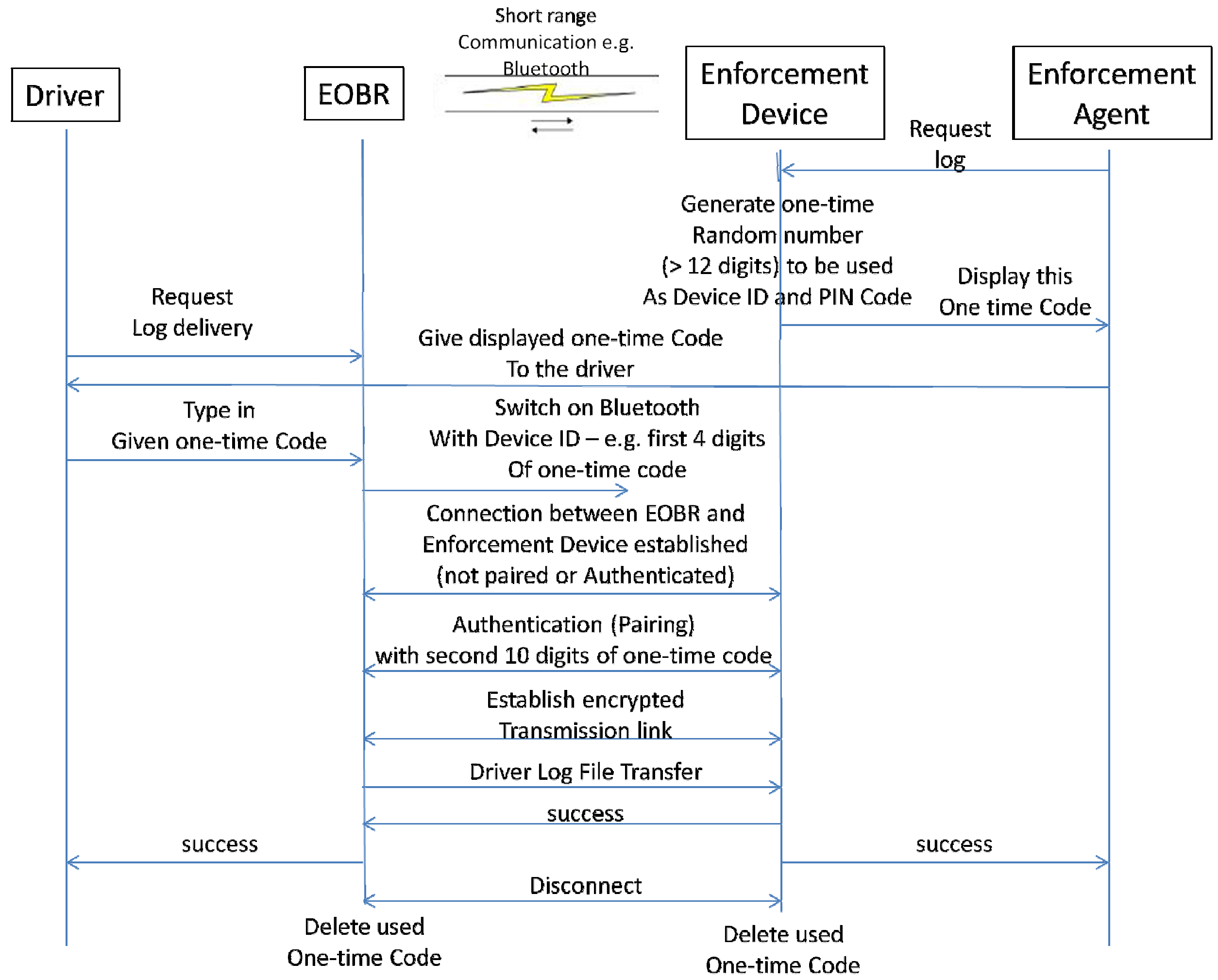


1. The enforcement agent requests an RODS file from the driver, who uses the EOBR to start the log delivery process.
2. The EOBR generates a one-time random number, which must be more than 12 digits. This number would consist of both the BT device name (e.g. first 4 digits) and the PIN (e.g. last 10 digits). The EOBR starts to transmit the device name.
3. The random number can be shown on the display of the EOBR and/or printed out via the integrated printer. The printout could contain just plain text or machine readable versions of the PIN e.g. bar code or QR code. The code can also be verbally given to the enforcement agent by the driver.

   The enforcement officer can directly observe that the driver is reading from, or has provided the printout from the EOBR being controlled.

4. The enforcement agent, using almost any bluetooth capable device as an enforcement device, and an appropriate application to configure the BT correctly, enters the whole random number either via scanning the printout or manually. The enforcement device can directly start to establish communication with the correct EOBR.
5. The two devices negotiate a stable physical connection, and enter the "connected" mode. At this point no authentication has taken place and data exchange is not yet possible.
6. Using the second part of the random number as the PIN, the two devices will perform the pairing operation and negotiate encryption keys. Now the communication is encrypted and secure, with the correct EOBR.
7. The RODS file is transferred from the EOBR to the enforcement device
8. If necessary the correct reception can be confirmed
9. The connection is then closed and the pairing information, including the random number (name and PIN) is deleted.

3.2.4 Internal BT connectivity with device name and authentication key generated by the enforcement device

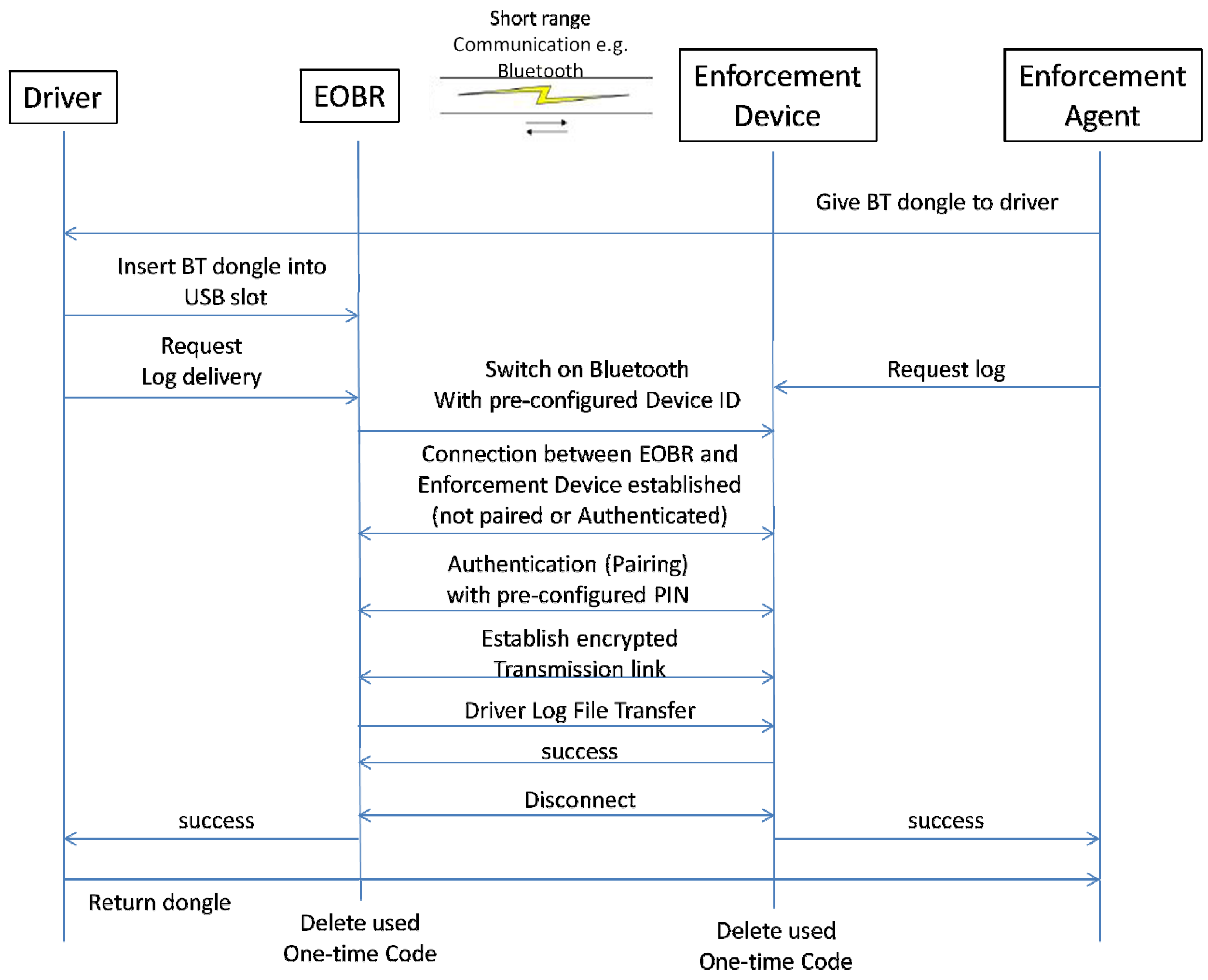


1. The enforcement agent uses the enforcement device to generate a one-time random number, which must be more than 12 digits. This number would consist of both the BT device name (e.g. first 4 digits) and the PIN (e.g. last 10 digits). The enforcement device starts to transmit the device name.
2. The enforcement agent requests an RODS file from the driver, who uses the EOBR to start the log delivery process.
3. The random number is shown on the display of the enforcement device and can be verbally given to the driver, or shown to the driver on the display of the mobile enforcement device.
4. The driver enters the random number into the EOBR. The enforcement officer can directly observe that the driver enters the number into the EOBR being controlled. This number is only

known to the two participants in the communication, not to a possible attacker. The EOBR can directly start to establish communication with the enforcement device.

5. Same as 3.2.3.
6. Same as 3.2.3.
7. Same as 3.2.3.
8. Same as 3.2.3.
9. Same as 3.2.3.

3.2.5 BT connectivity using pre-paired enforcement dongles


Short range
Communication e.g.
Bluetooth
Driver
EOBR
Enforcement Device
Enforcement Agent
Give BT dongle to driver
Insert BT dongle into USB slot
Request Log delivery
Switch on Bluetooth With pre-configured Device ID
Request log
Connection between EOBR and Enforcement Device established (not paired or Authenticated)
Authentication (Pairing) with pre-configured PIN
Establish encrypted Transmission link
Driver Log File Transfer
success
Disconnect
success
success
Return dongle
Delete used One-time Code
Delete used One-time Code

This scenario employs the use of a pre-configured BT dongle and a BT capable enforcement device. The BT dongle is not purely physical layer, but must support the authentication and encryption process. Such "cable-replacement" products are available at low cost.

1. The enforcement gives the driver a pre-paired BT dongle to insert into a USB slot provided by the EOBR. The BT dongle is pre-configured by the enforcement agency with the appropriate security settings, device names and PINs, which are unique to this pair of BT devices and stored persistently .
2. The driver inserts the dongle in the USB slot on the EOBR. The enforcement officer can directly observe that the driver enters the dongle into the EOBR being controlled.
3. The driver uses the EOBR to start the log delivery process. The enforcement agent uses the enforcement device to start the log reception process.
4. As the dongle and the enforcement device are already securely paired, the secure communication and data transfer can start without any further user interaction.
5. The RODS file is transferred from the EOBR to the enforcement device
6. If necessary the correct reception can be confirmed
7. The connection is then closed.
8. The driver returns the dongle to the enforcement officer.

This method of providing RODS files to an enforcement agent is highly secure, reliable and low cost. There are no language barriers to overcome, and no manual transfer of codes needed.

4. Advantages

Blue tooth technology was essentially developed to replace cables in small peer to peer environments. It is highly secure, and extremely cost effective. In some of the above scenarios, even a normal smart phone would fully suffice as an enforcement device.

This solution has virtually 100% availability, anywhere, anytime, regardless of internet and wireless connectivity, brownouts etc.

From a security point of view, the following properties are addressed:

- Authenticity/identification of EOBR: the enforcement agent to can visually ensure that the correct EOBR is being used for the data exchange
- Authentication of EOBR: Fundamental part of the BT protocol, using the pairing PINs provided.
- Non-repudiation of data: is not fully achievable without an appropriate signature on the data, either digital or via a signed printout. However, as the data can be demonstratively seen to have been downloaded directly from the driver's EOBR, and the connection is known to be secure, it is more difficult for the driver to successfully repudiate any infringements detected. A comparison of the data with a printout would further reduce the risk of repudiation.

- Integrity of data: the system does not provide any special mechanism to guarantee integrity, but the fact that a secure, encrypted peer to peer connection is established between a trusted EOBR and a trusted enforcement device, there is no opportunity for integrity loss due to manipulation.
- Confidentiality of data: is given by the secure, encrypted peer to peer connection with the trusted enforcement agent. This property is important to carriers to ensure that no other party than authorized enforcement agents have access to the vehicle routes and times. It will allow to include the full name of the driver in the RODS file and further enhance the non-repudation property of the system.

Using this solution could avoid the necessity to implement a public key infrastructure, while still providing an improved level of security.

As many mature off-the-shelf Bluetooth hardware and software solutions are available, implementing this mechanism would represent no schedule risk for the EOBR introduction.