Framework for Telematics Application Services Approach:

Prepared and submitted by a working group of the EOBR subcommittee, with participants including:

* David Kosiba, Qualcomm Enterprise Services, working group lead
* Scott Martin, Qualcomm Enterprise Services
* David Kraft, Qualcomm Enterprise Services
* Tom Cuthbertson, Xata
* Jim Angel, PeopleNet
* Doug Thompson, PeopleNet

This document is a work in progress and is intended to provide a baseline for discussions and further definition of the technical guidelines for electronic driver log file transfers using the recommended Telematics application services approach.

Contents

[Glossary 4](#_Toc306809254)

[References 4](#_Toc306809255)

[Log Transfer Overview 5](#_Toc306809256)

[Problem Statement 5](#_Toc306809257)

[Solution 5](#_Toc306809258)

[Architecture 6](#_Toc306809259)

[Multi-EOBR Host Vendor Support 7](#_Toc306809260)

[EOBR Communication Failure 8](#_Toc306809261)

[Distributed Portal Support 9](#_Toc306809262)

[Standardization 10](#_Toc306809263)

[Log Transfer Workflow 11](#_Toc306809264)

[Details of Log Transfer Workflow 12](#_Toc306809265)

[Requirements 13](#_Toc306809266)

[Security 14](#_Toc306809267)

[Overview 14](#_Toc306809268)

[Requirements 15](#_Toc306809269)

[PIN Format 15](#_Toc306809270)

[Overview 15](#_Toc306809271)

[Requirements 16](#_Toc306809272)

[PIN Timestamp and Log Data Scope 16](#_Toc306809273)

[Requirements 17](#_Toc306809274)

[Scope of data access 17](#_Toc306809275)

[Requirements 18](#_Toc306809276)

[PIN Expiry and Session Availability 19](#_Toc306809277)

[Requirements 19](#_Toc306809278)

[Data File Format 20](#_Toc306809279)

[XML Format 20](#_Toc306809280)

[Requirements 21](#_Toc306809281)

[Request and Response Interface 22](#_Toc306809282)

[Requirements 22](#_Toc306809283)

[Exception Handling 23](#_Toc306809284)

[Log File Transfer Request Errors (Normative) 23](#_Toc306809285)

[Miscellaneous Exceptions (Informative) 23](#_Toc306809286)

[Device Authentication Exceptions: 23](#_Toc306809287)

[Driver Authentication Exceptions: 24](#_Toc306809288)

[Driver Log Automation Exceptions 24](#_Toc306809289)

[Request for Electronic Log Data for Roadside Inspection Exceptions 24](#_Toc306809290)

[Driver Log File Generation Exceptions 24](#_Toc306809291)

[Mutual Authentications Exceptions 25](#_Toc306809292)

[Log File Transmitted and Acknowledged Exceptions 25](#_Toc306809293)

[Agent Retrieves / Receives Driver Log File Exceptions 26](#_Toc306809294)

[Inspection Completed Exceptions 26](#_Toc306809295)

[Miscellaneous Requirements 26](#_Toc306809296)

[Driver responsible for keeping logs up to date. 26](#_Toc306809297)

[Out of coverage scenario and Out of Band Log Transfer Request 27](#_Toc306809298)

[Implementation/Operational Requirements 27](#_Toc306809299)

[Timeouts 27](#_Toc306809300)

[Retry Policy 27](#_Toc306809301)

[Performance 27](#_Toc306809302)

[FMCSA Responsibilities 27](#_Toc306809303)

[Provisioning of EOBR Host URLs (Informative) 27](#_Toc306809304)

[Compliance and Certification 28](#_Toc306809305)

[Authentication Certificate Management 28](#_Toc306809306)

[Miscellaneous 28](#_Toc306809307)

[Appendix A – WSDL for SOAP log file transfer request and response 29](#_Toc306809308)

[Appendix B – XML Schema for log data file format 30](#_Toc306809309)

# Glossary

|  |  |
| --- | --- |
| EOBR | “Electronic On-Board Recorder”. Device for recording vehicle data including driver duty status changes. |
| FMCSA Portal | Centralized law enforcement portal used as the main access point for law enforcement officers to request and access driver log data for a roadside inspection. |
| EOBR Host | EOBR vendor back office system that talks to the EOBR units on the vehicles. |
| Mobile | EOBR unit onboard a vehicle |
| PIN | “Personal Identification Number”. A short sequence of alphanumeric digits used to identify a driver log. |
| XML | “Extensible Markup Language”. Industry standard set of rules for encoding documents in machine-readable form. Used extensively in business to business communications and data transfer. |
| B2B | “Business to business”. Commerce transactions between businesses. In our scenario this is a “data” exchange transaction. |
| WSDL | Web Services Description Language, the standard for defining Web Service interfaces. |
| XSD | XML Schema Definition, the standard for defining the format of any given XML file |

# References

|  |  |  |
| --- | --- | --- |
| XML 1.0 | XML Specification | http://www.w3.org/TR/REC-xml/ |
| TLS 1.2 | TLS specification | http://datatracker.ietf.org/doc/rfc5246/ |
| DD | 395.16 Data Dictionary | Appendix A – Table 2 – 395.16 Data Elements Dictionary |
| ISO 8601 | Data elements and interchange formats – Information interchange – Representation of dates and times | http://www.iso.org/iso/catalogue\_detail?csnumber=40874 |
| SEC1 | NIST Best practice standard | NIST SP (special publication) 800.52 for cert generation and management |
| SEC2 | Information Security Best Practices | TBD – recommendations for EOBR Host providers |

# Log Transfer Overview

## Problem Statement

Log file transfer is a transfer of data from vehicle EOBR system to EOBR Host system and then from EOBR Host system to an Enforcement Network Center or Portal via Web communications structure.

The goal of the this Telematics Approach for Log File Transfer is to provide ***unified solution for the secure transfer of driver log data to an Enforcement Portal***to allow Enforcement Officers performing roadside inspections to receive driver log data from a single trusted source. The Telematics approach is defined in this document to address the following areas of requirements:

* Provide a simple and timely process for an enforcement officer to request a electronic driver log file transfer and for the driver to initiate the process for the data transfer.
* Support for a single and/or distributed enforcement portal(s) receiving data from multiple distributed EOBR host vendors.
* Utilize standard commercially available Web services technologies for data transfers.
* Utilize standard commercially available security technologies for mutual authenticaitons and data encryption with data transfers.
* The solution SHOULD be resilient to bad data. It should allow for ease in detecting and handling data parsing problems and missing data.

## Solution

In order to meet the above requirements, the following components are a part of the proposed Telematics solution:

1. **Simple (6-digit) alphanumeric PIN code for identifying a driver log and for enforcement to use to request driver logs from the FMCSA Portal** – A PIN such as this is easy to remember and less likely to be a problem for enforcement with writing legibility, etc. And over time as the officer get accustomed to identifying the EOBR makes and models, the officers may only need to use 4 of the 6 digits making it even easier.
2. **A “Pull” mechanism for FMCSA Portal to retrieve driver log data from the EOBR Host system** – This allows for distributed portals and also enables FMCSA control over the process and reduces the risk of denial service attacks against the FMCSA portal.
3. **XML file format for data transfer** –This provides a standard, extensible, and widely used method for formatting data transfers. The rigid well-defined structure allows for easy detection of data problems during file validation when compared to fixed width or CSV file parsing (e.g. may not know you have a data problem until you try to process the data for simple fixed-width files).
4. **Simple (single request – single response) SOAP messaging scheme** – No need for extra communication to provide acknowledgements during the transfer process. The TCP layer will determine if transfer was successful and will handle retries and file reconstruction. The PIN code given from the driver to enforcement is the acknowledgement that the log request was a success. And Portal notification to the enforcement officer is the acknowledgement that the transfer was successful. *Note that we considered REST as an alternative, but expect that SOAP was more acceptable to Compass integration.*

## Architecture

The following diagram provides a visual of the logical components involved and the flow of data between them in a typical driver log transfer scenario. There are four main components of the overall architecture:

1. **EOBR Mobile** – Unit on vehicle that can initiate the request for a driver log transfer. Note that this is not mandatory as there may be other out of band methods to initiate the request (e.g. a call into dispatch). The critical point here is that the transfer of driver log data is initiated by the driver.
2. **EOBR Host (HOS)** – Backend system that receives the EOBR Mobile request for driver log transfer makes the driver log data available to Enforcement via the Enforcement Portal. The Telematics service provider (or EOBR Host system) manages information security of driver logs as recorded on the vehicle EOBR device, at the EOBR Host system, and between vehicle EOBR device and EOBR Host system.
3. **FMCSA Portal (Compass)** – FMCSA System that aggregates and hosts access to driver log data to Enforcement Officers.
4. **Enforcement Unit** – Application in Enforcement vehicle that can connect to the FMCSA Portal to request driver log transfer and display resulting logs, violations, etc. Roadside Enforcement Officer retrieves (pulls) data from the Portal and other network resource as data download becomes available.

The following diagram illustrates the overall workflow between these four main components.



1. Enforcement Officer stops vehicle at roadside inspection and requests the driver to initiate a request for log file transfer
2. Driver initiates the request for log transfer via EOBR
3. EOBR Host returns a PIN to pass to the Enforcement Officer to use when making the actual request for driver log data via the FMCSA Portal.
4. The driver gives the PIN to the Enforcement Officer.
5. The EOBR Host may store the PIN for future authorization verification when receiving the FMCSA Portal request.
6. The Enforcement Officer makes request to FMCSA Portal for retrieving the driver logs for the given PIN just obtained from the driver.
7. The FMCSA Portal makes a secure connection to the EOBR Host requesting the driver logs corresponding to the PIN entered by the Enforcement Officer via the FMCDA Portal.
8. The EOBR Host authorizes the request and returns the driver logs corresponding to the PIN generated from the original driver initiated request.
9. The FMCSA Portal makes the driver log data available to the Enforcement Officer.

## Multi-EOBR Host Vendor Support

The Telematics approach for driver log file transfer to Enforcement must support the ability to transfer data from multiple EOBR Host vendor systems to a single FMCSA Portal. The following set of diagrams illustrates how this proposed architecture supports multiple EOBR Host vendors.

The basic workflow is the same as the main architecture diagram above. However the critical aspect of the workflow is step 5 where the Enforcement Portal must look up the identity of the EOBR Host vendor based on the PIN in the incoming Log Request. As you will see in the requirements section below, in addition to the PIN identifying the driver for the log request, the PIN also identifies the EOBR Host vendor. Therefore the PIN returned by the EOBR Host and passed to the Enforcement Officer must contain the EOBR Host system identity.



So when a different EOBR Host system is used, the Enforcement Portal can look up the EOBR Host system identity and route the request to the appropriate vendor system.



## EOBR Communication Failure

Another nice to have with this Telematics solution is the ability to electronically transfer driver logs even if the vehicle EOBR is unable to communicate with the EOBR Host system. From the Enforcement Officer perspective it is the same workflow and is triggered by the receipt of the driver log PIN. The main difference here is the ability of the driver to call (out of band w.r.t. EOBR) a dispatch operator and request the generation of the driver log request PIN.

In this scenario, it is up to the dispatch company to verify the identity of the driver. Likewise it is up to the EOBR Host system to verify the identify of the user making the log transfer request via a Web interface to the EOBR Host system. But after these steps, the Enforcement Officer requesting the driver logs via the Enforcement Portal is identical to the above.



## Distributed Portal Support

This same architecture can support multiple distributed Enforcement Portals. Because of the pull nature of the data from the EOBR Host via the Enforcement Portal, as long as all the distributed Enforcement Portals are all provisioned with the proper security certificates and EOBR Host URLs, any Enforcement Portal may pull data from any EOBR Host system. The EOBR Host system doesn’t even (need to) know that the requests are coming from different portals.



## Standardization

The above architecture diagram includes many aspects that are not part of this standardization process. Those components that are not a part of the standardization process are up to the various parties (EOBR Host providers and the FMCSA Portal) to provide the implementation that meets the overall requirements. Specifically, the following diagram illustrates what part of this overall architecture we are standardizing, including :

1. WSDL interface for Enforcement Portal request to EOBR Host system for log retrieval
2. XML log file data format
3. PIN structure for EOBR vendor and driver log identification



Likewise, the components outside the starburst in this diagram illustrate those items that we are NOT standardizing, including:

* **Mobile to HOS host messaging for transfer request and PIN response** – It is up to the EOBR system implementation as to how this messaging takes place. If via EOBR to EOBR Host, any device to host authentication and authorization is out of scope of this section and is covered by other 395.16 requirements. In fact, this data flow could be completely out of band (e.g. via a Web UI on the EOBR Host system or even a phone call to the EOBR Host support team).
* **HOS host handling of request and PIN** – The management and storage of driver log transfer requests is completely up to the EOBR Host implementation. For example, if the Host vendor wishes to use a simple hash on driver ID, then there is no persistence of the PIN required, when the request comes in from the Enforcement Portal , that are able to extract the driver ID and deliver the logs for the specified driver. Likewise, the EOBR Host could simply use a random number as the PIN, and whenever a driver requests a log transfer, the host can generate a new random PIN and store it in a table of pending requests.
* **Request from Enforcement Vehicle to Enforcement Portal** – It is up to the FMCSA portal to give a simple mechanism for enforcement officers to make a log request and to enter the PIN. Likewise any officer authentication controls are also up to the FMCSA Portal to manage.
* **Storage of Driver Log data on the Enforcement Portal –** Any data retention and handling of the driver log data once on the FMCSA portal is completely up to the implementation of the FMCSA portal. The individual EOBR Host vendors have no control over what the FMCSA does with the log data once it is delivered. This is why the overall process is triggered by enforcement at a roadside inspection.
* **Notification to enforcement when driver log file available** – Since the enforcement officer interacts directly with the FMCSA Portal, it is up to this portal to handle notification of log availability to the requesting officer.
* **Data response to enforcement** – It is up to the Enforcement Portal as to the data format delivered to the Enforcement Officer. For example the Enforcement Portal could return a violations report back to the Enforcement Officer. Or on the other extreme, it could return the full set of driver log (raw) data to let an application on the Enforcement Officer’s unit process and determine any violations.

# Log Transfer Workflow

Based on the above architecture of the log file transfer, the following section details the typical workflow, including both the normal EOBR workflow as well as the roadside inspection log file request workflow.



*Note that based on the architecture diagram above, only steps 7, 8, and 10 in blue are Normative in this log transfer specification. All other steps are either informative, or are covered in other sections of the FMCSA specification.*

## Details of Log Transfer Workflow

The following descriptions each step of the process above.

1. Device Authentication (Out of scope) – Performance requirement that the host system authenticates all EOBR device connections to the host system.
2. Driver authentication (Out of scope) – Clarification of the performance requirement per 395.16 (j) *Driver Identification*. The performance requirement should include EOBR host system authentication of the driver ID and password or other biometric identifier.
3. Driver Log Automation (Out of scope) – Per the performance requirements of 395.16 and 395 Appendix A.
4. Request for Electronic Log Data for Roadside Inspection (Informative) – Request is a face to face interaction between enforcement agent and driver.
5. Driver request for transfer of logs to enforcement (Informative) – An EOBR function for driver initiation of electronic log transfer authorization. The function generates a file identifier (PIN) for the driver to convey to the enforcement agent.
6. Enforcement officer request for driver logs via portal (Informative) – An Enforcement Officer function that triggers the Enforcement Portal request for driver file transfer based on the PIN.
7. EOBR Host System Authentication (Normative) – An Enforcement Portal function that will initiate a secure connection with the EOBR host system following the trigger of the Enforcement Officer from step 6 above as per the Security requirements below in the section titled “Security”.
8. Portal Request to HOS system (Normative) – An Enforcement Portal function that requests the delivery of a driver log file. The Enforcement Portal request will follow the specified interface as given in the section below titled “Request and Response Interface” and also given by the WSDL in Appendix A.
9. Portal request authorization (Informative) – An EOBR Host function that ensures that the Enforcement Portal request is for a valid driver that has previously requested transfer of his log data. How the EOBR host system authorizes the request (e.g. validates the PIN in the request) is up to implementation. However the implementation MUST only respond with data for requests from the Portal where the driver initiated the request.
10. Driver Log File Transmission (Normative) – An EOBR host function for delivery of previously requested driver log data. Formatting of the log download will be accomplished by the host system and will include:
    1. Driver log data generation per field definitions as specified in 395.16 Appendix A.
    2. The file will be formatted using the XML standard and is defined by the XSD given in Appendix B.
11. Agent Retrieves / Receives Driver Log File (Informative) – The agent is expected to have connectivity with the enforcement portal and will be alerted when the file is available. It is assumed that information security is managed by the enforcement systems (e.g. Portal and client application) and no additional requirements are needed.
12. Inspection Completed (Informative) – As closure, the inspection is completed with no violation, or with initiation of another process to deal with the violation.

## Requirements

**[REQ]** The EOBR Host system SHALL support secure connections from the Enforcement Portal to enable secure transfer of the driver log data. For detailed security requirements, see “Security” section below.

**[REQ]** The EOBR Host system SHALL support SOAP-based Web Service requests for the method defined by the WSDL file defined in Appendix A.

**[REQ]** The EOBR Host system SHALL support delivery of the driver log data in a valid XML format according to XSD file defined in Appendix B.

# Security

## Overview

The only security elements being specified here is the actual transfer of the driver log data from the EOBR Host system to the Enforcement Portal system. In order to transfer this log data securely, both the EOBR Host and the FMCSA Portal will utilize TLS authentication as the means of establishing a secure channel for the transfer of data [TLS 1.2]. Specifically, they will use client-authenticated TLS to ensure that both parties are mutually authenticated. And all the data transmitted within the TLS session will be encrypted with industry-standard encryption as part of the secure channel established by the TLS session [TLS 1.2].

Client-authenticated TLS connection requires both the EOBR Host System and the Enforcement Portal to possess certificates by the FMCSA. FMCSA is responsible for managing certificates with all the EOBR Host vendors authorized to provide electronic driver log file transfers.

The specific authentication and encryption resources to be applied are to be specified by FMCSA. However it is recommended that the encryption scheme selected during the cipher suite negotiation part of the TLS handshaking is AES-128.

The FMCSA should follow certificate management best practices [SEC1] when creating and managing the storage and delivery of these certificates. In addition, the FMCSA should create independent server certificates to be delivered to each authorized EOBR Host vendor. Likewise, in the single centralized FMCSA Portal model, the EOBR Host systems should only accept (or be provisioned with) a single FMCSA client certificate.

In the case of multiple distributed FMCSA enforcement portals, the EOBR Host systems should only accept (or be provisioned with) a list of accepted FMCSA enforcement portals. In addition, the FMCSA, when generating the certificates for the distributed portals, should create a master certificate from which all child certificates are created and installed on the distributed enforcement portals.

**Question:** Does the EOBR Host also need to have the FMCSA master cert for validating the child client certs?

When distributing the certificates to the EOBR Host vendors, the FMCSA should follow security best practices in the delivery of the certificates [SEC1], for example via electronic transfer via PGP encrypted email, via physical medium (e.g. flash drive), or in person.

*Note that currently TLS 1.2 is supported in Windows Server 2008 R2 and on Windows 7. However, only TLS 1.0 is natively supported Windows Server 2003. And so far it does not look like there is a hot fix from Microsoft to enable TLS 1.2 on 2003.*

TBD – EOBR Host vendor recommendations for information security best practices (other NIST standards) [SEC2]

## Requirements

**[REQ]** The EOBR host system SHALL support client-authenticated TLS connection from the Enforcement Portal.

**[REQ]** Since the transfer of log data is a pull from the FMCSA Portal system, the EOBR host system shall act as the “TLS Server” in the TLS handshake and the FMCSA Portal shall act as the “TLS Client”.

**[REQ]** The client-authentication TLS connection SHALL be established according to TLS 1.2 Specification [TLS 1.2]

**[REQ]** The EOBR Host SHALL at a minimum support AES-128 as one of the possible TLS cipher suites.

**[REQ]** If the connection establishment is not successful (e.g. connection drops before success), the FLCSA Portal (TLS client) SHALL establish a new session on every connection. It is NOT mandatory that the EOBR Host systems support the shortcut mechanism for resuming TLS handshake.

**[REQ]** The transmission of the SOAP request and response bodies SHALL be encrypted by the secure connection established by the TLS connection requirement above.

**[REQ]** The EOBR host system SHALL reject any request where TLS authentication fails (e.g. without valid certificates)

TBD – checking on other optional items in TLS that we may want to recommend.

# PIN Format

## Overview

As shown in the above architecture diagram, the driver log request generates a specific PIN value that the Enforcement Officer uses to make the request to the FMCSA Portal. This PIN identifies the EOBR Host company (e.g. Qualcomm, Xata, PeopleNet, others) for the FMCSA Portal to know where to route the request for driver logs.

In addition to identifying the EOBR host company, the PIN must also encapsulate the unique driver/company identity, as this PIN ins the only information used by the FMCSA Portal to make request for driver logs. To accomplish this two-fold requirements, we propose the following PIN format:



The PIN number is a simple alphanumeric number that can be easily conveyed from the driver to the Enforcement Officer. The first two digits of the PIN are an alphabetic code identifying the EOBR host provider (e.g. “QC” for Qualcomm, “XT” for Xata, “PN” for PeopleNet, etc.). And the remaining 4 digits are up to the host provider implementation.

It is recommended that the mobile display the company identifier and remaining 4-digit code separately in the EOBR interface. This may make it easier for enforcement to take the code from the driver and enter in the FMCSA portal. For example, as enforcement officer become more familiar with the EOBR vendor units, they may no longer need the first two digit company identifier. They will automatically know that the unit is from vendor “XX”. Then all the officer really needs to get from the driver is the remaining 4-digit code identifying their logs.

## Requirements

**[REQ]** The PIN format SHALL be six (6) alphanumeric characters

**[REQ]** The PIN format SHALL be case agnostic (upper and lower case treated the same)

**[REQ]** The PIN format SHALL NOT contain any special characters (e.g. commas, parenthesis, etc.)

**[REQ]** The first two characters of the PIN SHALL be assigned by the FMCSA registry for each EOBR host system hosting company.

**[REQ]** The first two characters of the PIN SHALL be alphabetic characters ONLY.

**[REQ]** The remaining 4 characters of the PIN are up to EOBR Vendor implementation to define the usage.

# PIN Timestamp and Log Data Scope

The PIN represents a very specific instance in time up to which the driver’s logs should contain log data. More specifically, when logs are requested for a PIN, it should only generate log data that was “on the EOBR at the time of the PIN request”. For example, if a PIN were generated by a driver request at 6:34PM, the resulting driver log file should only contain driver log data up through 6:34PM. Even if the enforcement officer request through the FMCSA Portal was at 7:04PM, the log data should only contain data up through 6:34PM.

To accommodate this, an EOBR Host implementation may attach a timestamp to each PIN code that is generated. This timestamp could then be used when delivering the data to the FMCSA portal.

A subtle nuance of this requirement is that any back office driver log data edits that were made before the PIN request, but that have not yet been received by the EOBR, SHOULD NOT be included in the driver log data delivered to the FMCSA portal. Therefore the statement above, “should only generate log data that was on the EOBR at the time of the PIN request” should be taken very literally. EOBR Host implementation must take care not to include data that was not yet received by the mobile when delivering to the FMCSA portal.

Note that there is a nuance around multiple PIN requests in the same roadside inspection. When the first PIN is requested, this sets the exact timestamp of the “snapshot” of EOBR data to be delivered. Multiple successive PIN requests (e.g. every 5 minutes) should generate the exact same log. Any back office edits made during the roadside inspection period should NOT be included, even if a followup PIN request was made after the back office edit was made.

## Requirements

**[REQ]** Driver log file data delivered to the FMCSA portal SHALL ONLY contain data that was on the EOBR at the time the PIN request was initially made.

**[REQ]** Driver log file data delivered to the FMCSA portal SHALL NOT contain data that may have been added after the time at which the PIN request was made (e.g. a back office edit of a log record that was not yet received at the EOBR, even if for the same time period).

**[REQ]** If an enforcement officer makes additional PIN requests to the driver in the same roadside inspection, the “snapshot” of the data provided SHALL be the same as that for the original PIN. The log data returned SHALL NOT take into account any new data since the first PIN request.

# Scope of data access

As mentioned above, the data returned by the EOBR Host is up to the time at which the PIN request was made (e.g. a snapshot of what was on the EOBR at the time the PIN request was made). However, this does not specify how far back in time to go (e.g. if an EOBR happens to store more data than is required by law).

The beginning of the data returned in the log file delivered to the FMCSA portal should be the “start of cycle” [[1]](#footnote-1) driver and it should contain either 7 or 8 days depending on the driver rule set. So for a driver on the 7-day rule, the data should include the current day and go back 6 days. But for a driver on an 8-day rule, the data should include the current day and go back 7 days.

For cases where the first duty status goes beyond the previous 6 or 7 days (e.g. started before and continues through midnight), the driver log file should contain the actual start time of that duty status, even though it technically falls outside of the 6- or 7-day window. For example, the following diagram shows the case where the first duty status (“Driving”) spans the start of day (assuming midnight).



In this case, the first event in the driver log file should contain the actual start time of the Driving event, and not artificially have the start time of midnight. This would produce a log file with the following events. *Note that this example uses local time and not UTC for illustrative purposes*:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Doe | John | 12345 | **20111024** | 17:30 | 1 | D |
| Doe | John | 12345 | 20111025 | 01:00 | 2 | SB |
| Doe | John | 12345 | 20111025 | 09:00 | 3 | ON |
| Doe | John | 12345 | 20111025 | 10:30 | 4 | D |
| … | … | … | … | … | … | … |

Likewise, for any duty statuses that span the terminal start of day, the events should not be artificially split at midnight. So to continue the log data file example, for duty statuses that span the terminal start of day, you would have the following log file data:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| … | … | … | … | … | … | … |
| Doe | John | 12345 | 20111025 | 09:00 | 3 | ON |
| Doe | John | 12345 | 20111025 | 10:30 | 4 | D |
| Doe | John | 12345 | 20111025 | 09:00 | 5 | ON |
| Doe | John | 12345 | 20111025 | 20:00 | 6 | OFF |
| Doe | John | 12345 | 20111026 | 03:00 | 7 | ON |
| … | … | … | … | … | … | … |

As an implementation note, if the EOBR Host system internally splits duty statuses at the terminal start of day, if must combine them back together into a single event before sending the log to the FMCSA portal.

## Requirements

**[REQ]** For drivers on a 7-day rule, the EOBR Host system SHALL include driver log data for the current day plus the previous 6 full days.

**[REQ]** For drivers on a 8-day rule, the EOBR Host system SHALL include driver log data for the current day plus the previous 7 full days.

**[REQ]** When calculating a full day, the EOBR and Host SHALL use the terminal start of day for which the driver is associated. Note that this MAY not be midnight.

**[REQ]** For the first event in the log (e.g. going back the 6 or 7 days), if the event spans the terminal start of day (e.g. the actual start time of the event was before the start of day on the first day), the event log should contain the actual start time of the event, and not artificially indicate the start time as the terminal start of day.

**[REQ]** The dates and times in the event data SHALL be in UTC time according to the Data Dictionary [REF]

# PIN Expiry and Session Availability

Since the driver log data is intended to be used for roadside inspection by enforcement, the PIN code used to identify the driver log data is only valid for a short period of time. After such time, the PIN will no longer provide enforcement access to that specific driver log data for that instance in time and the PIN is said to have “expired”. Once a PIN is expired, the enforcement officer must request the driver to request a new PIN to obtain the driver’s log data.

## Requirements

**[REQ]** When assigning a PIN to a log request by a driver, the EOBR host system MUST NOT reuse a PIN that is currently active (that has not yet expired) by another log request. All active PIN “sessions” must be unique.

**[REQ]** The EOBR Host system SHALL keep all log file request PINs active for a value of XXX minutes (to be defined by FMCSA – default of 15 minutes with a max of 1 hour). After such time, the PIN is no longer valid and data is not available form the EOBR Host system.

**[REQ]** If a request for an expired PIN is received, the EOBR SHALL respond with the appropriate error code indicating that the PIN has expired. See the section on “Exception Handling” below for specific error codes.

**[REQ]** The EOBR Host system MAY remove data availability after the FMCSA Portal has successfully pulled the data (e.g. even if still within the availability window defined above).

**[REQ]** The EOBR Host system implementation SHOULD attempt to conceal the algorithm of generating the PIN. For example, the PIN should not simply be a monotonically increasing number that is easily guessable.

# Data File Format

The driver log data file will be formatted in XML for ease in parsing and error handling by the FMCSA portal. As mentioned above, the rigid well-defined structure of XML allows for easy detection of data problems during XML file validation when compared to fixed width or CSV file parsing (e.g. may not know you have a data problem until you try to process the data for simple fixed-width files).

However, note that you must “escape” certain “special characters” when placing them in XML files. For example, you cannot have a single apostrophe character (‘) within an XML formatted file. This single character must be converted to (&apos) when represented in an XML file. There are other special character handling rules defined by [XML 1.0] that must be followed.

The XML structure of the data file format follows the same basic elements defined in the FMCSA Data Dictionary [DD]. However we have added two new elements that were missing from the Data Dictionary, the driver rule set and the terminal start of day. These two additional elements are described in the following sections.

## XML Format

The following is an example XML structure of the data to be included in the driver log transfer response. The actual format will be governed by the XSD definition given in Appendix B.

<DriverLogData>

<EventList>

<Event>

<DriverIdentificationData>

<DriverFirstName/>

<DriverLastName/>

<DriverID/>

**<Ruleset/>**

**<TerminalStartTime/>**

</DriverIdentificationData>

<VehicleIdentificationData/>

<CoDriverData/>

<CompanyIdentificationData/>

<ShipmentData/>

<EventData/>

</Event>

<Event/>

...

</EventList>

</DriverLogData>

## Requirements

**[REQ]** The XML data file format SHALL conform to the XSD file given in Appendix B.

**[REQ]** The <DriverLogData> element SHALL contain one and only one <EventList> element.

**[REQ]** The <EventList> element SHALL contain a sequence of one or more <Event> elements.

**[REQ]** The <Event> element SHALL contain exactly one each of the following elements, <DriverIdentificationData>, <VehicleIdentificationData>, <CoDriverData>, <CompanyIdentificationData>, <ShipmentData>, and <EventData>.

**[REQ]** The data elements SHALL follow the type and data size requirements specified in [DD]

**[REQ]** The < DriverIdentificationData > element SHALL contain all of the “Driver Identification Data” data elements in Table 2 – EOBR Data Elements Dictionary [REF] plus two additional elements, <Ruleset> and <TerminalStartTime>.

**[REQ]** The <Ruleset> element SHALL contain the 7\_DAY or 8\_DAY designation according to the XSD definition in Appendix B.

**[REQ]** The <TerminalStartTime> element SHALL contain UTC time in ISO 8601 format [ISO 8601] of start of day for the driver’s home terminal (e.g. [YYYY][MM][DD]T[hh][mm]Z.)

**[REQ]** The <VehicleIdentificationData> element SHALL contain all of the “Vehicle Identification Data” data elements in Table 2 – EOBR Data Elements Dictionary [DD].

**[REQ]** The <CoDriverData> element SHALL contain all of the “Co-Driver Identification Data” data elements in Table 2 – EOBR Data Elements Dictionary [DD].

**[REQ]** The <CompanyIdentificationData> element SHALL contain all of the “Company Identification Data” data elements in Table 2 – EOBR Data Elements Dictionary [DD].

**[REQ]** The <ShipmentData> element SHALL element SHALL contain all of the “Shipment Data” data elements in Table 2 – EOBR Data Elements Dictionary [DD].

**[REQ]** The <EventData> element SHALL contain all of the “Event Data” data elements in Table 2 – EOBR Data Elements Dictionary [DD].

**[REQ]** The <SequenceID> element contained within the <EventData> element SHALL be a continuous monotonically increasing value for driver throughout the entire 7-8 day log transfer data.

**[REQ]** The <SequenceID> element SHALL be tied to the driver for the entire series of events in the driver log file and is NOT tied to the vehicle and/or day as currently specified in the Data Dictionary [DD].

# Request and Response Interface

The request/response for delivery of the driver log from EOBR host system to the enforcement portal is via SOAP (Simple Object Access Protocol). The request takes the 6-digit PIN but broken into two parts, the EOBR Vendor identifier, and the 4-character-code (4CC) log identifier.

The actual request XML is documented via a separate WSDL file given in Appendix A. But an example of the XML payload of the SOAP request (e.g. the SOAP Body) is given below:

<FMCSALogTransferRequest>

<RequestVendorCode/>

<RequestPIN4CC/>

</FMCSALogTransferRequest>

The request contains a single top-level XML element <FMCSALogTransferRequest>. The two-part PIN elements are contained inside this main element. Both of the PIN elements are mandatory in the request. The vendor code is used by EOBR host vendor to verify that the request was to the proper EOBR Host vendor. And the PIN four character code is needed by the EOBR Host to uniquely identify the driver log request.

The response contains a single top-level XML element <FMCSALogTransferResponse>. The response will echo both the requested vendor code and 4CC PIN elements as well as a single container element that holds the driver log data. . In addition it will respond with the number of days cycle that the driver is on, indicating how many days of logs are in the response.

<FMCSALogTransferResponse>

<ResponseStatus/>

<RequestVendorCode/>

<RequestPIN4CC/>

<DriverLogData/>

</FMCSALogTransferResponse>

## Requirements

**[REQ]** The <FMCSADriverLogRequest> SHALL contain both the vendor code and 4-character-code log identifiers.

**[REQ]** The <FMCSADriverLogResponse> SHALL contain a status element, echo both the vendor code and 4-character-code log identifiers, plus contain a single <DriverLogData> container for the log data.

**[REQ]** The <ResponseStatus> element SHALL contain an indication of the status of the request/response as per the Exception Handling section below.

**[REQ]** The <DriverLogData> element SHALL contain the data elements as per section XXX above and as described in the Data Dictionary [DD].

# Exception Handling

This section discusses various exception scenarios and provides guidance on how to handle them.

## Log File Transfer Request Errors (Normative)

This section provides the supported response and error codes from the EOBR Host system in response to a log file transfer request from the Enforcement Portal. The following table lists the responses, error codes and any recommended actions to be taken by the enforcement officer.

|  |  |
| --- | --- |
| **<ResponseStatus/> value** | **Recommended Action** |
| SUCCESS | * Log transfer was successful and response contains full 7 or 8 days worth of driver logs |
| PARTIAL\_DATA | * Driver log data does not contain the full 7 or 8 days worth of log data. * Enforcement to verify with driver if a new driver, and to check for paper logs for missing days. |
| PIN\_EXPIRED | * Enforcement Officer to verify PIN with driver * If valid, Enforcement Officer request driver to make a new log transfer request to generate a new PIN |
| PIN\_NOT\_FOUND | * Enforcement Officer to verify PIN with driver * If PIN still not found, enforcement to request a new PIN from driver |
| INVALID\_PIN | * PIN may not be a valid format (e.g. may contain unsupported characters) * Enforcement Officer to verify PIN with driver |
| INVALID\_EOBR\_COMPANY | * If the first two digits of the PIN to not match the EOBR host company. Likely due to an incorrect configuration of the Enforcement Portal URLs. * Officer to verify PIN with driver * If same, Officer to call Enforcement Portal support line |
| Others TBD | * TBD |

Note that there may be other error responses from the FMCSA portal failing to connect to the EOBR Host provider, or other general failure scenarios. These responses would include standard HTTP error codes, any TLS handshake errors, etc. These are out of scope of this document and any response from the FMCSA Portal to the enforcement officer should take these errors into account. The section below on miscellaneous exceptions gives some recommendations on how to handle some of these scenarios.

## Miscellaneous Exceptions (Informative)

The following are some miscellaneous exception handling scenarios (Informative):

### Device Authentication Exceptions:

|  |  |
| --- | --- |
| **Exception** | **Recommendation** |
| Out of coverage and authentication not completed. | * EOBR continues to function to record driver logs but records are identified as subject to device authentication. * Log downloads cannot be initiated by a device not connected and authenticated by the EOBR host system. |
| Device authentication failed. | * Driver alerted of sensor failure and the need to record paper RODS * Continued automated recording subject to resolution of sensor failure and recovery issue. Recommend that EOBR continues to function to record driver logs but records are identified as subject to device authentication. If authentication is restored, then records accepted. If authentication not restored, manual logs must be processed. * Log downloads cannot be initiated by a device not authenticated by the EOBR host system. |

### Driver Authentication Exceptions:

|  |  |
| --- | --- |
| **Exception** | **Recommendation** |
| Out of coverage and authentication not completed. | * EOBR continues to function to record driver logs but records are identified as subject to driver authentication. * Log downloads cannot be initiated until EOBR connected and driver authenticated by the EOBR host system. |
| Driver authentication failed. | * Driver alerted of access denied for EOBR use and the need to record paper RODS. * Continued automated recording of all vehicle movement and any sensor failure events. * Log downloads cannot be initiated by a driver not authenticated by the EOBR host system. |

### Driver Log Automation Exceptions

|  |  |
| --- | --- |
| **Exception** | **Recommendation** |
| Sensor or EOBR system failures resulting in drivers recording paper RODS. | * Driver only able to provide electronic logs for time period with no sensor or EOBR failure. * Driver must provide paper logs for remaining time period |

### Request for Electronic Log Data for Roadside Inspection Exceptions

|  |  |
| --- | --- |
| **Exception** | **Recommendation** |
| Driver provides incorrect file identifier to enforcement agent resulting in file not found by agent. | * Recommend that EOBR provide a re-display of file name (PIN) used. |
| No connectivity | * View on device * Backup plan XXXXX * Backup to paper logs |
| EOBR Host Downtime | * TBD * Standard world of system downtime * Not only place for manual process (e.g. connectivity end to end) |

### Driver Log File Generation Exceptions

|  |  |
| --- | --- |
| **Exception** | **Recommendation** |
| Gaps in log data. | * Driver had prior duty status events where paper RODS used. * Driver had prior duty status events in other vehicle with 395.15 compliant AOBRD where data has not been applied to EOBR currently in use. * Recommend that at a minimum driver is alerted of all gaps in electronic log as recorded on EOBR currently being used. Subject to resolution of issue on log data integration, recommend also that driver and back office make best effort attempt to provide integrated electronic records for complete driver log. |
| Annotated records on EOBR host system not applied to EOBR currently in use. | * Back office annotations to correct driver errors (e.g., driver failed to enter off-duty when taking a break). * Back office annotation to apply corrections to driver violation of company policy (e.g., driver entered off-duty for break when not authorized to be off-duty). * Back office entry of driver other work that was otherwise recorded as off-duty (e.g., driver work in warehouse or work with other employer). * Recommend that driver is alerted of all back office annotations to log records. Subject to resolution of issue on log data integration, recommend also that driver and back office make best effort attempt to provide integrated electronic records for complete driver log. Alternatively, recommend that EOBR provide a display of all back office annotated records. |
| EOBR host system not available | * Driver may be detained for some period waiting for log download. |

### Mutual Authentications Exceptions

|  |  |
| --- | --- |
| **Exception** | **Recommendation** |
| Authentication fails | * Recommend that FMCSA portal services provide 24x7x365 support to resolve authentication failures on a timely basis. Support services also to provide timely resolution for persistent connection failures and recovery of system availability if portal system fails. * Recommend that EOBR host system service providers be required to disclose their hours of support to their customers and FMCSA portal services support center. |
| FMCSA enforcement portal not available | * Recommend that FMCSA establish and achieve a service level agreement that will support the needs of the enforcement community for access to driver log downloads for roadside inspection. |
| EOBR Host System not available | * Recommend that EOBR host system service providers be required to disclose their hours of support to FMCSA portal services support center. |

### Log File Transmitted and Acknowledged Exceptions

|  |  |
| --- | --- |
| **Exception** | **Recommendation** |
| Connection fails during file transmission | * Recommend that FMCSA service provide automatically detect connection failure and trigger restart of connect, authentication, and file transmission process. |
| Acknowledgement not received. | * Recommend that service provide automatically if acknowledgement not received in defined time period and trigger restart of connection, authentication, and file transmission process. * Recommend that FMCSA portal services and EOBR host system services provider each provide 24X7X365 support to resolve file transmission failures on a timely basis. |

### Agent Retrieves / Receives Driver Log File Exceptions

|  |  |
| --- | --- |
| **Exception** | **Recommendation** |
| Agent cannot connect and/or authenticate with FMCSA portal | FMCSA and/or state enforcement agencies should establish a remote support services function to leverage review of electronic log data via voice support to roadside inspections. The roadside agent remains responsible for violation determination and enforcement, but is assisted as the support service provides input based on review of the driver’s electronic log data pertaining to:   * Verification of authenticity of log displays and/or printouts available at roadside based on log summary data of system identifying information  (i.e., check on potential counterfeit log printouts or log display system in driver possession). * Confirmation or disproval of determination of violation for complex log data scenario. * Identification of log data abnormalities and information gaps to be substantiated further through manual inspection based on detailed data analysis of GPS positions (with map interface), event status data, and record annotation details. |
| Enforcement device cannot process downloaded file |
| Enforcement device provides different interpretation of driver log data than EOBR (e.g., violation determination on one system but not the other) |
| Agent does not have device or operating device to receive downloads. |

### Inspection Completed Exceptions

|  |  |
| --- | --- |
| **Exception** | **Recommendation** |
| Inspection not recorded in SMS |  |

# Miscellaneous Requirements

## Driver responsible for keeping logs up to date.

As mentioned above, any back office driver log data edits that were made before the PIN request, but that have not yet been received by the EOBR, SHOULD NOT be included in the driver log data delivered to the FMCSA portal. Therefore if there are edits that are required to get the logs current and accurate, it is the driver’s responsibility to request updated logs before submitting the log transfer PIN request.

In addition, when a driver makes the PIN request for transfer of driver logs, this should also trigger the driver’s current duty status to revert to “On Duty” (if the automatic change in duty status from driving has not yet been applied).

## Out of coverage scenario and Out of Band Log Transfer Request

If the EOBR is not able to make the request to the EOBR host system (e.g. stops along roadside out of coverage or COMM problems, the driver is subject to the requirements as defined for manual inspections.

# Implementation/Operational Requirements

## Timeouts

The FMCSA should provide the timeout values for which the FMCSA Portal operates. The individual EOBR Host vendors should ensure that their systems can operate within these constraints.

## Retry Policy

Since it is a PULL request from the MFCSA to each HOS provider, the retry logic is up to the FMCSA Portal. For example, if the first request by the FMCSA portal times out waiting for a response, it is up to the portal as to initiating any retries.

The EOBR Hosts should support accepting retry requests that have not yet been successfully completed. However it is not expected that the EOBR Host systems will honor maliciously performing requests. Based on operational security policies, the EOBR Host systems may start executing DoS policies.

## Performance

Overall cycle time from log download initiation to receipt by the enforcement device is expected to be approximately a few minutes assuming no exceptions in the process.

# FMCSA Responsibilities

## Provisioning of EOBR Host URLs (Informative)

The FMCSA needs to maintain a registry of HOS providers and a mapping to the HOS Hosting Company Identifiers. How the FMCSA Portal is provisioned with and manages the different EOBR Host URLS is outside the scope of this specification. However it is conceivable that the FMCSA Portal keeps a simple list of EOBR Vendor Identifier to URL mapping as shown in the following table.

|  |  |  |
| --- | --- | --- |
| Company Key | URL | Company |
| QC | https://myqualcommapps.com/QHOS/FMCSALogTransfer.asmx | Qualcomm |
| XT | https://xata.com/HOS/FMCSALogTransfer | Xata |
| PN | https://www.peoplenet.com/fmcsa/hos/logTransfer | PeopleNet |
| … | … | … |

Whenever a new EOBR Host vendor registers with the FMCSA, the FMCSA should allocate a new 2-digit Company Identifier to that vendor.

## Compliance and Certification

FMCSA is responsible for establishing a testing environment to verify transfer of log data files. In addition to testing the SOAP messaging and data file format in the response, this testing will also include test certificates to validate the TLS mutual authentication.

The FMCSA is responsible for coordinating (or subcontracting this function) certification testing among all registered EOBR Host vendors. Once an EOBR vendor certification test has passed, the FMCSA will give a TLS authentication certificate to the EOBR vendor.

## Authentication Certificate Management

FMCSA will provide certificate authority services and generate public and private key certificates for each EOBR Host System and each Enforcement Portal. The FMCSA should follow certificate management best practices [SEC1] when creating and managing the storage and delivery of these certificates.

FMCSA will provide, support, and manage authentication credentials with EOBR Telematics service providers and carriers as operators of their own EOBR host system. In addition, the FMCSA should create independent server certificates to be delivered to each authorized EOBR Host vendor. In the case of multiple distributed FMCSA enforcement portals, the FMCSA should create a master certificate from which all child certificates are created and installed on the distributed enforcement portals.

When distributing the certificates to the EOBR Host vendors, the FMCSA should follow security best practices in the delivery of the certificates [SEC1], for example via electronic transfer via PGP encrypted email, via physical medium (e.g. flash drive), or in person.

FMCSA may revoke authentication credentials for any EOBR Host service provider that does not provide log download files per specified requirements or does not perform on a timely and reliable basis.

## Miscellaneous

FMCSA will provide and manage the enforcement portal services.

NOTE that expectation is ERODS will handle any DST days issues. All timestamps in the data file format are in UTC time.

# Appendix A – WSDL for SOAP log file transfer request and response

TBD

# Appendix B – XML Schema for log data file format

TBD

1. This is typically the “start of day” of the terminal to which the driver is associated. For a private fleet driver it would be the driver’s main terminal. But for a for-hire driver this value may only be a reference to home terminal time. [↑](#footnote-ref-1)