Risks and Problems associated with a Telematic Approach for Log Downloads for EOBRs

Revision 1.0

Continental
6755 Snowdrift Road
Allentown, PA 18106
+1 (610) 289-0488

Table of Contents

1. Introduction 3
2. Summary 3
3. Risk Analysis 4
   3.1 Lack of data integrity protection 4
   3.2 Lack of authenticity of data 4
   3.3 Repudiation possible 4
   3.4 High Level of Complexity 4
   3.5 Availability of enforcement infrastructure 5
   3.6 Availability of wireless network 5
   3.7 Key and Certificate Infrastructure 5
   3.8 Transaction and communication costs 5
4. Glossary 6
   4.1 Integrity 6
   4.2 Authenticity 6
   4.3 Authentication 6
   4.4 Repudiation 6

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 contains feedback on the potential risks and obvious problems associated with the concept described in the document *Framework for Telematics Application Services Approach--DRAFT.DOCX* and presented by Qualcomm, Xata and PeopleNet at the MCSAC meeting on 25.10.2011.

2. Summary

There are considerable risks associated with the exclusive usage of a multi-node telematic system for the transmission and storage of electronic driving records for EOBR devices. The following factors represent the main risk elements in terms of security, usability, costs and availability:

- Lack of data integrity protection
- Lack of authenticity of data
- Repudiation possible (rejection of records by driver or fleet as invalid)
- High level of complexity
- Availability of enforcement infrastructure
- Availability of wireless network
- Key and certificate Infrastructure
- Transaction costs

This document is not questioning in any way the attainable security level using state of the art transmission technologies e.g. SSL, VPN, that are correctly implemented and use an appropriate, reliable trust anchor. The focus is more on the steps between the secure transmissions and the insecure storage of data, as well as the complexity of the resulting system and the costs incurred for all involved stakeholders.

Furthermore, Continental strongly recommends the separation of **legal** EOBR and **commercial** Fleet Management Systems (FMS) requirements. A ruling that mandates only peer to peer roadside inspections would give FMS manufacturers the freedom to continue to develop the needed commercial FMS solutions for their customers while avoiding the cost and complexity of the proposed telematic enforcement solution. The EOBR application can clearly be integrated in an FMS product, but the EOBR requirements should not be influenced by FMS implementations.

3. Risk Analysis

3.1 Lack of data integrity protection

The lack of data integrity protection is a major concern of the proposed telematic solution. Despite the fact that authentication and secure transmission is employed between the different nodes of the system, there is no secure mechanism employed to ensure that the original data (electronic driving records) cannot be changed, or to detect changes once they have occurred. This allows the data to be changed, either deliberately or due to human or computer error, at the following stages of the process:

- *Within the EOBR Host System*: it would easily be possible to modify driving records to either increase the available driving time or to avoid infringement detection.
- *Within the Enforcement System*: main risk due to human error or system errors.
- *Within the Roadside Enforcement Device*: main risk due to human error or system errors.

This issue can be fully mitigated using the solution proposed by Continental in the document *EOBR_Security_Concept_Proposal_v1.0.pdf.*

3.2 Lack of authenticity of data

Similar to the data integrity issue, is the ability of the roadside agent to be certain that the electronic driving records which have been provided actually come from the EOBR and the driver being controlled. This cannot be guaranteed by the proposed telematic system, as the data itself carries no secure information linking it to the source EOBR. Secure communication of the data from one insecure storage node to another, cannot provide the needed assurance.

The cryptographic mechanisms commonly employed to provide integrity, also provide the necessary authenticity.

3.3 Repudiation possible

Due to the above points describing the lack of data integrity and authenticity protection, in an infringement situation, the involved driver could repudiate his actions. Holding the driver accountable for the infringements would be problematic as it very difficult to prove that the data has not been modified, and that there have been no system errors that could potentially lead to incorrect data being delivered to the roadside agent.

This weakness would be common knowledge amongst drivers within a short space of time, and could be exploited in infringement situations.

3.4 High Level of Complexity

The 30 page document *Framework for Telematics Application Services Approach--DRAFT.DOCX* clearly demonstrates the high level of complexity that roadside enforcement using a telematic approach incurs. There are many scenarios involved, all of which require significant infrastructure to be put in place and

maintained. Apart from the increased costs, this will make the system less robust and reduce its availability. This will lead to fewer roadside inpections being completed.

3.5 Availability of enforcement infrastructure

For the proposed telematic solution to be usable nationwide, all enforcement agents would need to be equipped with appropriate enforcement computers, all of which must be wireless and internet capable.

Depending on the current penetration of such equipment, this represents a significant investment as well as recurring maintenance and training costs for the enforcement community.

3.6 Availability of wireless network

Fleet management applications are generally insensitive to the lack of wireless connectivity in extended areas – it is likely that a connection will be available later on the route.

However, with a telematic solution, roadside controls in an area in which wireless connections to the internet are not available or not reliable will be difficult or impossible. This contradicts the basic federal requirement that a driver must be able to present his driving records to law enforcement upon request.

3.7 Key and Certificate Infrastructure

The telematic based solution proposes that the FMCSA should provide, support and manage authentication credentials ("*FMCSA is responsible for managing certificates with all the EOBR Host vendors authorized to provide electronic driver log file transfers*"). This PKI (public key infrastructure) is only used to secure the communication between the nodes of the telematic system and incurs costs for all involved.

In other words, this increased cost would be a direct result of the use of a telematic based enforcement approach and would provide little or no added value to the security of the total EOBR system.

The provision of key infrastructure and a PKI implementation is justified when applied down to the level of the EOBR devices which would achieve a significantly higher security level for the whole system. Such a PKI implementation would be compatible with both a peer-to-peer or a telematics approach. This approach is detailed in the solution proposed by Continental in the document *EOBR_Security_Concept_Proposal_v1.0.pdf.*

3.8 Transaction and communication costs

A telematic based enforcement solution would incur significant monthly fees and per usage costs for carriers for communications, data handling and storage. Law enforcement agencies would also have to bear such costs. A peer-to-peer based solution would completely avoid such costs.

4. Glossary

4.1 Integrity

Integrity is the property that data is protected against inadvertent or unauthorized modification.

4.2 Authenticity

Authenticity is the property that data is genuine and originated from its purported source

4.3 Authentication

Authentication is the process of establishing confidence in user identities.

4.4 Repudiation

Claiming to have not performed an action. Repudiation occurs when someone performs an action and then claims that they didn't actually do it.