NTRCI
NATIONAL TRANSPORTATION
RESEARCH CENTER, INCORPORATED
University Transportation Center

Project U22: Trusted Truck® II (Phase D)

This project was funded by the NTRCI University Transportation Center under a grant from the U.S. Department of Transportation Research and Innovative Technology Administration (#DTRT06G-0043)

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the Department of Transportation University Transportation Centers Program, in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof.

George Bitar, Thomas Richter, Paul Muschick, Sandra Selley Volvo Technology
Itamar Arel, Andrew Davis, Anuradha Bulusu University of Tennessee

October, 2010

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.

4. Title and Subtitle **U22: Trusted Truck® II (Phase D)**	5. Report Date **October 2010**
	6. Performing Organization Code
7. Author(s) **George Bitar, Thomas Richter, Paul Muschick, Sandra Selley - Volvo Technology** **Itamar Arel, Andrew Davis, Anuradha Bulusu - University of Tennessee**	8. Performing Organization Report No.
9. Performing Organization Name and Address **National Transportation Research Center, Inc.** **University Transportation Center** **2360 Cherahala Blvd.** **Knoxville, TN 37932**	10. Work Unit No. (TRAIS)
	11. Contract or Grant No. **DTRT06G-0043**
12. Sponsoring Agency Name and Address **U.S. Department of Transportation** **Research and Innovative Technology Administration** **1200 New Jersey Avenue, SE** **Washington, DC 20590**	13. Type of Report and Period Covered **Final Report August 2009-October 2010**
	14. Sponsoring Agency Code **RITA**

15. Supplementary Notes

16. Abstract

The Trusted Truck® Independent Certification System is a wireless roadside inspection initiative that offers immediate and vital incentives to the vehicle operator to save the many hours spent waiting in line at state vehicle inspection stations, while at the same time giving the state inspection authorities a much higher volume of vehicle inspections than possible at current staffing levels. The adoption of this concept on our highways will provide for operators a dramatic and welcome increase in efficiency, and for inspection authorities the same welcome increase in the number of vehicles inspected.

Phase D is the culmination of the Trusted Truck® project, which has successfully delivered a full working prototype, and a live demonstration of this unique concept.

In Phase D, high level data security was implemented to provide the exchange of encryption certificates per inspection between the truck and the Trusted Truck® Management Center. This included an optimization specific to this application, designed and published by the University of Tennessee. Another major feature delivered was the “Pre-Trip” inspection feature that allows operators to detect out of compliance items at any time to facilitate convenient repair. This same feature can be used by inspection authorities to manually determine if the system is providing true indications.

The project delivered the specifications and background information needed for franchisees to instantiate a Trusted Truck® Management Center. This information includes a Concept of Operations, which describes, among other items, the system architecture used to implement the vehicle and server applications. The information also includes a definition of the Certificate of Trust used to qualify compliant vehicles.

The final demonstration was held in August 2010, and was attended by the two US Congressmen, Representative James Oberstar of Minnesota, Chairman of the Congressional Committee on Transportation and Infrastructure, and Representative John Duncan of Tennessee.

17. Key Word Trusted Truck® II, wireless roadside inspections, commercial vehicles, safety regulations, encryption	18. Distribution Statement **No restrictions**

19. Security Classif. (of this report) **Unclassified**	20. Security Classif. (of this page) **Unclassified**	21. No. of Pages **58**	22. Price

Table of Contents

List of Tables

List of Figures

List of Definitions

ACRONYM	DEFINITION
ATA	American Trucking Association
ATRI	American Transportation Research Institute
CMRS	Commercial Mobile Radio Service
CMV	Commercial Motor Vehicle
CVSA	Commercial Vehicle Safety Alliance
DES	Data Encryption Standard
DSRC	Dedicated Short Range Communications
FMCSA	Federal Motor Carrier Safety Administration
EOBR	Electronic On-Board Recorder
FOC	Fleet Operations Center
GPS	Global Positioning System
GSM	Global System for Mobile communications
HMI	Human Machine Interface
HOS	Hours of Service
NHTSA	National Highway Transportation Safety Administration
NOK	Not OK - A negative condition or response (the opposite of "OK")
NTRCI	National Transportation Research Center, Inc., University Transportation Center
OBC	On-Board Component - The hardware and software in the vehicle
OBE	On-Board Equipment
OEM	Original Equipment Manufacturer
SDMS	Safety Data Message Set
TCP/IP	Transmission Control Protocol / Internet Protocol
TTMC	Trusted Truck® Management Center
TTMS	Trusted Truck® Message Set
UDP	User Datagram Protocol
UT	University of Tennessee
VIN	Vehicle Identification Number
VTEC	Volvo Technology
VTEC-US	Volvo Technology Corporation-United States
VMS	Volvo Message System
Volpe	John A. Volpe National Transportation Systems Center
WCF	Windows® Communication Foundation
WRI	Wireless Roadside Inspection

Executive Summary

The Trusted Truck® Independent Certification System is a wireless roadside inspection initiative that offers immediate and vital incentives to the vehicle operator to save the many hours spent waiting in line at state vehicle inspection stations, while at the same time giving the state inspection authorities a much higher volume of vehicle inspections than possible at current staffing levels. The adoption of this concept on our highways will provide for operators a dramatic and welcome increase in efficiency, and for inspection authorities the same welcome increase in the number of vehicles inspected.

Phase D is the culmination of the Trusted Truck® project, which has successfully delivered a full working prototype, and a live demonstration of this unique concept.

The concept was built and demonstrated in four phases over a six year period.

- In Phase A the minimum required inspections items such as tire pressure, lighting and brake condition were implemented, along with the first vehicle and server applications needed to support them.
- In Phase B, driver authentication, and axle weight inspection features were added. Tractor to trailer communication was implemented to include the core inspection items for the trailer, and to include cargo security. In addition, the initial specifications for system architecture were delivered.
- In Phase C, the system architecture was finalized, along with details of the message set that would be used. Low-level data security (encryption) was implemented to prevent data-tampering and offer the fleets assurance that sensitive data could not be intercepted by competitors.
- In Phase D, high level data security was implemented to provide the exchange of encryption certificates per inspection between the truck and the Trusted Truck® Management Center. This included an optimization specific to this application, designed and published by the University of Tennessee. Another major feature delivered was the "Pre-Trip" inspection feature that allows operators to detect out of compliance items at any time to facilitate convenient repair. This same feature can be used by inspection authorities to manually determine if the system is providing true indications.

The final demonstration of the Trusted Truck® project, held in August 2010, was attended by the two US Congressmen, Representative James Oberstar of Minnesota, Chairman of the Congressional Committee on Transportation and Infrastructure, and Representative John Duncan of Tennessee. The demonstration used a heavy-duty class 8 tractor-trailer to exercise wireless inspections for two cases, one in which the vehicle was in compliance, and then a case which detected non-compliance. As the vehicles completed the inspections, the attendees observed live

inspection data displayed on the inspection control panel inside the prototype Trusted Truck® Management Center.

The project delivered the specifications and background information needed for franchisees to instantiate a Trusted Truck® Management Center. This information includes a Concept of Operations, which describes, among other items, the system architecture used to implement the vehicle and server applications. The information also includes a definition of the Certificate of Trust used to qualify compliant vehicles. Phase D successfully delivered Trusted Truck® in its prototype form, giving the WRI community a service uniquely positioned to provide certain benefits, including:

- A reduction of processing time for wireless inspection data on government servers
- An incentive for industry buy-in, due to the buffering of sensitive data
- A means for the generally compliant fleets to avoid inspection delays, without enabling punitive measures for a failed inspection
- An opportunity for fleets to use a “Pre-Trip” function and know that vehicle is compliant before departing
- The option for the government to request non-required data, if allowed by the fleet
- The possibility for fleets to go online and evaluate their compliance level against the overall population

Given these benefits, and the fact that the concept is adaptable to the various wireless data-collection schemes that will be used in various jurisdictions, Trusted Truck® distinguishes itself as the one WRI enabler that allows the trucking industry to maintain a stake in the regulation of their own compliance.

Chapter 1 – General Overview

Background

The states conduct close to 750,000 roadside inspections of commercial vehicles per year. Even with this seemingly large number of inspections, the states are still being overwhelmed with the burden of performing inspections in a fashion that ensures the carriers are complying with safety regulations without impacting the profitability of the carriers. In the first Trusted Truck® project, Volvo helped demonstrate the ability to perform brake inspections wirelessly between the vehicle and the state's roadside infrastructure.

The first two phases of the Trusted Truck® II project built off of that initial project to further explore the concept of building a relationship of trust with commercial vehicles and motor carriers through wireless roadside inspections and compliance, along with ways that would help enhance the efficiency of the carriers. The goal was to move closer to defining a mechanism for performing wireless roadside inspections (WRI).

The final two phases of the Trusted Truck® II project were focused on realizing the complete system in its final form. The goal was to develop, deliver and demonstrate the system as a working prototype.

Project Team

The Trusted Truck® project team was led by the National Transportation Research Center, Inc., University Transportation Center, and included the University of Tennessee, and Volvo Technology North America.

The Trusted Truck® concept was conceived and refined based on discussions with Class 8 heavy duty truck drivers and fleets with the notion of improving safety while at the same time improving operational efficiency. Both the NTRCI and Volvo Trucks North America conducted these discussions which also included developing and understanding of the goals of the US DOT as well as enforcement agencies. NTRCI led the team in ensuring that the Trusted Truck® concept was developed both as a viable component of and in concert with the goals of the FMCSA wireless roadside Inspection (WRI) project. NTRCI in collaboration with the team members made an assessment of available and developing technology to determine the best course of action.

The University of Tennessee, Knoxville (UT) brought expertise in weigh station operations as well as the insight into all government relevant databases and software applications used by the state and federal enforcement community. Additionally, they developed the security protocols as part of the encryption strategy for all data exchanged between the various entities during a wireless roadside inspection (WRI). They also were instrumental in finalizing the TTMC applications.

Volvo Technology (VTEC) provided project management, and developed most of the software applications needed to realize the Trusted Truck® concept. VTEC took the lead in writing the Concept of Operations, the System Requirement Specification, and the System Architecture documents. VTEC designed, and assembled the On-Board hardware systems. VTEC designed and developed the on-board software applications, the Fleet Operations Center applications, and provided initial development of the TTMC application. The VN780 tractor and 53' trailer were supplied by VTEC and instrumented with the help of Volvo Trucks North America.

Project Description

Trusted Truck® Vision

The Phase D vision was demonstrated in August 2010 and displayed the concept of a nationwide system to improve the efficiency of roadside inspections. The goal was to meet the needs of state and federal regulators to improve road safety, security and efficiency while also providing incentives to fleet owners and drivers to adopt the system.

This vision was realized by developing a working prototype of the Trusted Truck® Independent Certification System. Specific goals included the following:

- Develop and demonstrate a *state specific* "Certificate of Trust" validating the tractor, trailer, driver and/or load.
- Develop a working prototype of a TTMC including an interface to the VOLPE/FMCSA WRI back office.
- A secondary goal is to access additional data from the FMCSA back-office, demonstrating the interface in simulated form if necessary, as a fallback.
- Demonstrate the full concept using the Certificate of Trust.
- Outreach to Volvo/Mack customers and contacts to determine their needs and obtain feedback on the concept

Deliverables

In addition to the actual demonstration, all project output was required to be available for government and industry informational inquiries. Detailed records of this work would enable potential TTMC franchise holders to assess market entry. The Phase D deliverables are comprised of a final demonstration, artifacts of the final demonstration, and a video documenting the entire Trusted Truck® concept.

A final demonstration of the Trusted Truck® concept was held on August 13, 2010, at NTRCI in Knoxville, Tennessee. The objective of the demonstration was to exercise the entire system in front of representatives from Government and industry. While the truck proceeded on a prescribed test route, live data was displayed to the audience inside the prototype Trusted Truck®

Management Center. The demonstration was successful in showing two inspection scenarios, one for the case of a “trusted” vehicle, and one for the case of a non-compliant vehicle.

Key artifacts of the final demonstration include the presentation entitled ‘Trusted Truck® Overview and Demonstration’[1] and video footage taken during the event. VTEC also supported NTRCI in development of the ‘Trusted Truck®’ informational pamphlet which was made available at the event.

A video was produced which documents the entire Trusted Truck® concept[2]. The video begins with the 1st Trusted Truck® project in 2003-2004 and continues through Phases A, B, C, and D of the Trusted Truck® II project, culminating with the August 13, 2010, final demonstration in Knoxville, TN. The purpose of the video is to communicate the overall Trusted Truck® concept to fleets, industry, and government while emphasizing the benefits accompanying this unique approach to wireless roadside inspections.

[1] The presentation can be found at this link:http://www.ntrci.org/library/Trusted_Truck_AUG_13_2010-Demonstration_1289846027.pdf

[2] The video can be found at this link:http://www.ntrci.org/libraries/video.html

Chapter 2 – Research Methodology

Volvo/Mack Brand Outreach

During development of the Trusted Truck® concept it was felt that for its successful implementation the Trusted Truck® Certification system must be independent of both the government and individual heavy duty truck original equipment manufacturers (OEM). It should function as an independent third party to provide a confidential interface between drivers and carriers and the government. Yet the state and federal government enforcement agencies must also have confidence that its functioning is in keeping with all regulations. For that reason the team also felt that the third party provider of the Trusted Truck® Certification system must be both certified and audited by the government. Only in this way can both parties to the system (operators and government) have confidence that valid wireless inspections are being conducted and data is being protected.

Validation of the belief of the team that the system should be independent of an OEM was validated by Volvo Technology North America. In January 2010, the Trusted Truck® concept was discussed internally at Volvo between Volvo Technology of America and the Volvo and Mack brand organizations. The key items discussed were regulations, competitive position and time to market, and creating added value to maximize the benefit.

One main point of discussion was consideration that an OEM should not become directly involved in TTMC ownership. This stems from the fact that a conflict of interest could arise where loyal OEM customers are being represented to the inspection authorities.

Ssafety and brand recognition is a key element to the OEMs interest in Trusted Truck®. Any OEM that strives to be associated with highway safety, the development of the Trusted Truck® Certification System presents an opportunity to validate their brand image. If the OEM can offer features that create a smoother transition for customers into the realm of wireless inspection, they can leverage the time-saving benefits into additional vehicle sales.

Encryption Strategy

Need for Standard Security

For any system, such as Trusted Truck®, that would be widely adopted, there will be considerable effort made to keep the system “off the shelf”. This is true of the data security work that was performed. All data security work was based on the Data Encryption Standard (DES) set forth by the National Institute of Standards and Technology.

To use this technology to its fullest potential requires, on a per use basis, an exchange of security certificates between parties. Thus, per vehicle inspection, the TTMC® and truck exchange security certificates, and generate a new security key to encrypt the inspection data. This insures that TTMC® and truck are guaranteed to be the valid transmitters and receivers of data that is sensitive to operators and OEMs.

Consideration of Legacy On-Board Systems

Because the data security computations can become intensive for brief periods, there was further consideration regarding lower-power on-board hardware that might be present on older vehicles, or in lower-cost offerings. Thus, the on-board software implementation was made compatible with less-powerful, 16-bit processors. Converting the algorithm from a 32-bit, to a 16-bit implementation allowed a wider group of target hardware to be used. This step was important in order to keeping initial costs low for operators.

Need for Efficient Calculations

When a truck, or any other type vehicle enters the inspection zone, there is a limited time to establish communications, perform the inspection, and receive the result. The objective of this work was to employ standard DES algorithms, and then optimize them to trim valuable time from the operation. The processing for the dynamic key generation, that occurs on-board the vehicle, was decomposed and reconstructed to allow some of the processing to be done prior to the beginning of the certificate exchange. This would allow the vehicle to complete an inspection, and immediately perform pre-calculations in preparation for the next inspection.

To ensure that the computations that enable the encryption scheme are executed in a timely fashion on the truck's hardware, the Chinese Remainder Theorem (CRT) was utilized to evaluate the modular exponentiation for signature generation. By utilizing the CRT, a 16-bit system is able to compute the signature approximately three times faster. This topic is discussed in depth in Appendix C – “A Data Security Protocol for the Trusted Truck® System”.

Additional Over the Air Messages

The message scheme for over-the-air messages used in phases A, B, and C, required only the transmitting of the inspection message, and the response. Because in Phase C the encryption key was “fixed” (the same for any session) that message sequence did not need to expand.

In Phase D, security certificate management was required in the TTMC and the OBE. This was required because it allowed 2 critical capabilities. First, the TTMC and OBE could receive certificates and verify the identity of endpoint with whom sensitive data is exchanged. Second, these security certificates contain a signature from which the encryption key can be derived dynamically, that is, per inspection.

The message sequence used in the wireless inspection is described in Figure 1.

Pre-Departure Inspection

The Pre-Departure Inspection function was implemented to provide a means for drivers to trigger a wireless inspection prior to departure (i.e. not within a geofence), and determine that the truck is in compliance. A fleet could require these activities before and after each drive and thus collect statistics for their own use.

This Pre-Departure Inspection can also be useful as part of a technical audit process, whereby the authorities can fault a particular component, trigger an inspection manually, and retrieve the expected result, thus verifying an accurate response from the TTMC and OBE.

The addition of this function in the OBE required the augmentation of the text and images displayed on the monitor in the truck. This function thus allows the driver to trigger the self-inspection from the truck, and later see the response from the TTMC. The response is presented on a monitor in the form of a “laundry-list” that itemizes all out-of-compliance vehicle components.

The inspection message that arrives at the TTMC needed to be augmented as well. The TTMC needs to know if an incoming inspection message is a self-inspection, or one that has been triggered by entering an inspection zone. This is a key indicator, in that self-inspections should not cause any indication of trusted status to the government server, or any communication with an inspection station.

Over-The-Air Message Sequence

The message sequence used in the wireless inspection is described in Figure 1. Noteworthy is the fact that the primary trigger that initiates the inspection can occur due to entry of a geofence area, or entry to a local area network, or by other means, as new technology becomes available. In this way and in many others, the Trusted Truck® Certification System maintains independence with respect to the implementations that will be found in different inspection jurisdictions.

In the case of the geofence trigger, the vehicle is constantly receiving position data via the GPS satellite network, and is constantly performing calculations to determine if its current location falls into one of the designated geofence inspection zones. Thus, within seconds of entering the geofence area, the vehicle will proceed with the inspection sequence.

In the case of the local area network, the vehicle will arrive within a DSRC-capable network, and once the network system ID is verified, proceed with the inspection sequence.

The technology used for triggering the inspection, can be treated independently of the technology used to send the messages. Once the inspection is triggered, the messaging itself can take place over various communication means. The type of communication, and number of alternative methods available in any instance is limited only by the equipment available on the vehicle and the network.

An inspection authority (i.e. state government) may require that triggering take place via DSRC, but that does not dictate the technology used for the subsequent messaging. Even though DSRC is capable of transmitting the inspection messages, that authority may require that messaging then occurs via a different technology, for example CMRS (GSM, CDMA, etc.). It is even technologically feasible that once the inspection is triggered, the vehicle may be allowed to determine its preferred technology based on cost.

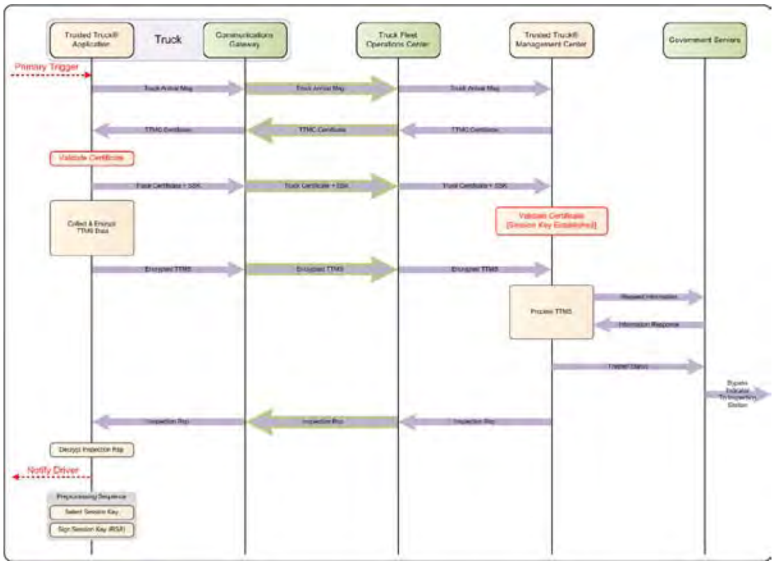


Figure 1. Diagram. Trusted Truck® Message Sequence

The Video

The video serves to document the entire Trusted Truck® concept. Action Video was brought in to document the entire final demonstration, augmented with key interviews, an explanation of the concept, and footage of presentations and speeches. This video will serve as a tool to introduce government officials, operators, and OEMs to the concept, as well as a resource to be viewed by potential operators of a Trusted Truck® Messaging Center when considering potential business opportunities.

Interface with Volpe/FMCSA

On behalf of FMCSA, there is an effort underway at the John A. Volpe National Transportation Systems Center to define a government database that could provide records on file with various governments, regarding transportation. The project team wanted to show the concept of obtaining additional attributes about a vehicle and driver from a federal database. UT implemented a bidirectional interface between the TTMC and a simulated Volpe server. During the demonstration, a computer application was used to simulate the government server, and take part in the inspection.

Inbound queries to the Volpe server take the form of requests for CDL status, and any applicable Out-of-Service restrictions that might exist, and be needed to validate the drivers credentials. This first contact would be limited to a query, and would occur at a point in the inspection process before the TTMC has determined trust. Outbound information from the Volpe server would thus be used to transact the certificate of trust.

Once trust was determined, the TTMC would send the certificate of trust to the Volpe server to indicate that a “trusted” truck was bypassing an inspection station. This certificate would be used to record credit for a given inspection to the respective inspection station. In addition credit could be given to the driver and fleet to enhance the BASIC score for CSA2010 compliance.

The Demonstration

The final demonstration occurred at the end of Phase D, and was performed on August 13, 2010, at NTRCI, located in Knoxville, TN, with the objective of exercising the entire system in front of representatives from Government and industry. In attendance were the two U.S. Congressmen, U.S. Rep. James L. Oberstar of Minnesota, chairman of the Committee on Transportation and Infrastructure, as well as U.S. Rep. John J. Duncan Jr., ranking member of the Highway and Transit Subcommittee. Also in attendance were representative from US Department of Transportation, FMCSA, NHTSA, CVSA, ATA, ATRI and other transportation sector organizations.

Figure 2. Photograph. Trusted Truck® Final Demonstration. Shown in the foreground are Joe Petrolino, Vice President of Heavy Vehicle R&D, NTRCI, and Rep. James Oberstar

The demonstration required the truck to follow a pre-defined route upon which the truck systems would automatically trigger, based on location, gather the required data electronically, and transmit it to the TTMC, which was operating in the demonstration conference room, and being viewed by the invitees. It is important to note that the message path also included the FOC (located in Greensboro, NC), the Government Server (simulated), and the Bypass Notifier. The Bypass Notifier is an application that represents the view to be seen at the inspection station. The inspection sequence is shown in Figure 3.

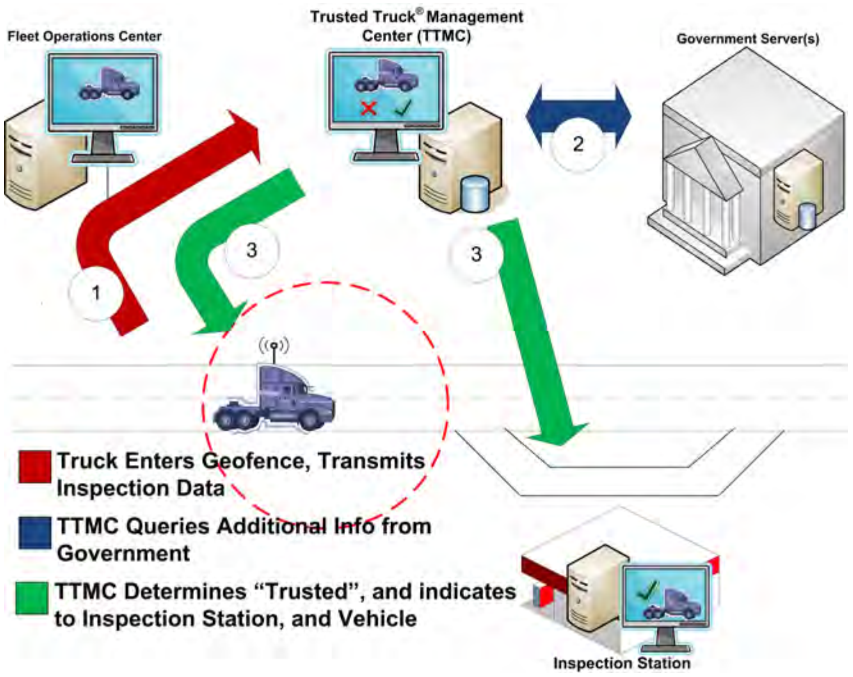

Fleet Operations Center
Trusted Truck® Management Center (TTMC)
Government Server(s)
1
2
3
3
🟥 Truck Enters Geofence, Transmits Inspection Data
🟦 TTMC Queries Additional Info from Government
🟩 TTMC Determines "Trusted", and indicates to Inspection Station, and Vehicle
Inspection Station

Figure 3. Diagram. Trusted Truck® Inspection Sequence

The demonstration included two inspection instances, one for the case of a "trusted" vehicle, and one for the case of a non-compliant vehicle. Upon entering the approach zone the first time, the truck received a positive result ("You may bypass the weigh station" appeared on the in-dash display). Before entering the approach zone for the second pass, the fire extinguisher sensor was detached, at which the truck failed the wireless inspection ("Please Enter the Weigh Station" appeared on the in-dash display), and the TTMC graphical user interface displayed all truck data, and flagged the fire extinguisher as being out of compliance. The TTMC, wireless inspection and approach zones are shown in Figure 4.

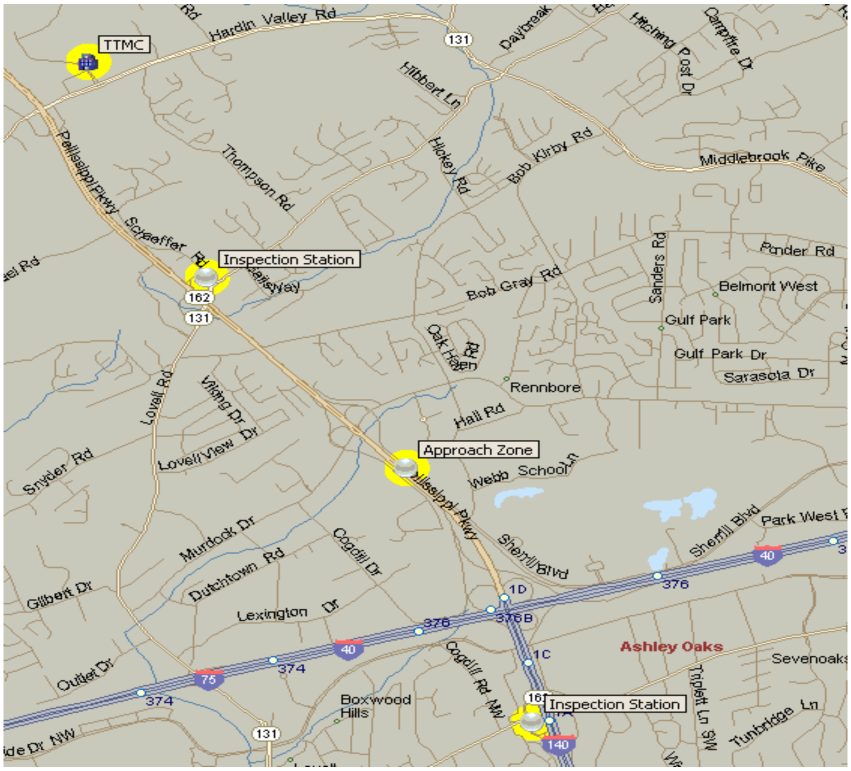
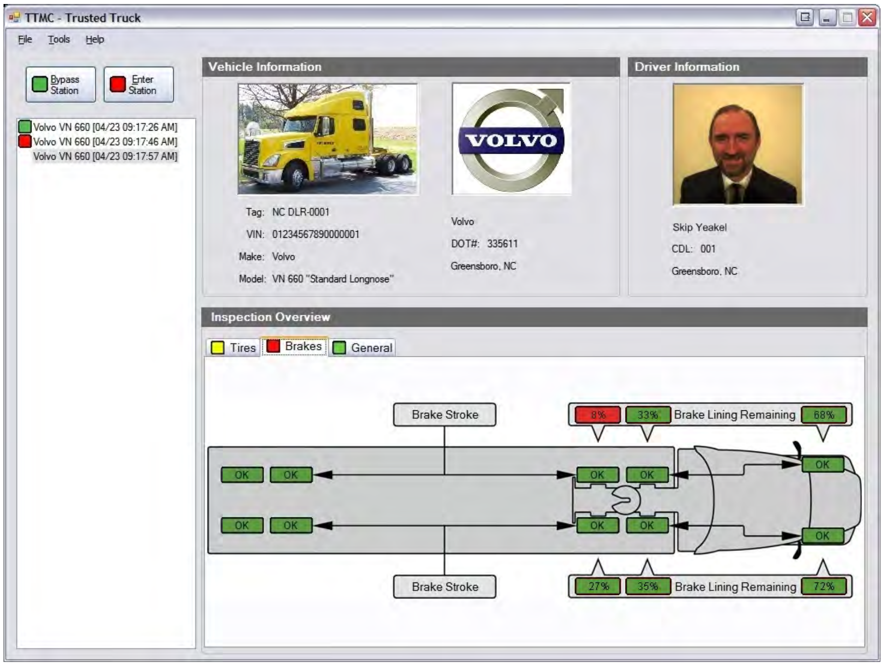


Figure 4. Map. Wireless Inspection Zone, and Inspection Stations

Each time the truck transmitted the inspection message, the data would subsequently appear at the TTMC, filling the various portions of the user interface (Figure 5).



🟩 Volvo VN 660 [04/23 09:17:26 AM]
🟥 Volvo VN 660 [04/23 09:17:46 AM]
Volvo VN 660 [04/23 09:17:57 AM]

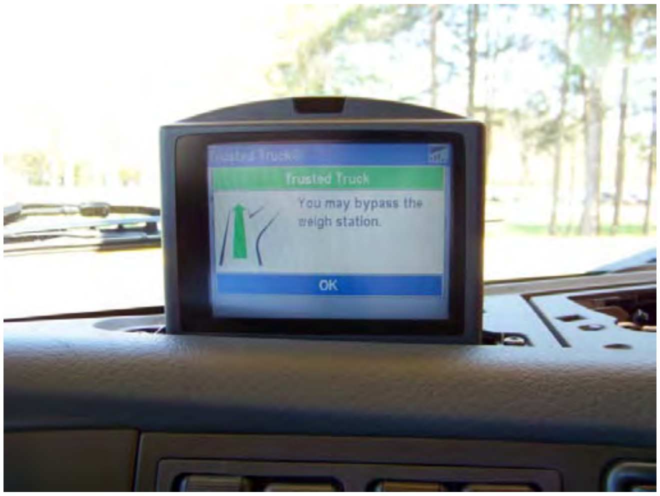
Tag: NC DLR-0001
VIN: 01234567890000001
Make: Volvo
Model: VN 660 "Standard Longnose"

Volvo
DOT#: 335611
Greensboro, NC

Skip Yeakel
CDL: 001
Greensboro, NC

Figure 5. Screen Shot. TTMC User Interface, Brake Status Panel

The driver would, at the completion of each wireless inspection, receive an indication to bypass or enter the inspection station, via the in-dash display (Figure 6).



You may bypass the weigh station.

Figure 6. Photograph. Truck In-Dash Display

Chapter 3 – Concept of Operations

The concept of operations will be stated generically in the sections that follow, but additional information is available elsewhere in this document, predominantly in the System Requirements Specification. Trusted Truck® can be viewed in terms of need, features, advantages, and the role of the stakeholders. The following descriptions provide the essential points for each view.

Concept Overview

The Need For Trusted Truck®

In the future, the government may require wireless vehicle inspections for chronic violators, and encourage it for all. If this comes to fruition, then the industry needs a “buffer” to manage the flow of sensitive data. Additionally, there is a need for an intermediary to gain industry buy-in, and government acceptance. Trusted Truck® was designed to fill this role.

Trusted Truck® Management Center

The TTMC is a third-party provider of data-management between the FMCSA and any FOC. As a benefit to industry, it is the one solution that provides a buffer for sensitive fleet and driver data. The TTMC indicates only if that vehicle satisfies requirements (i.e. trusted status). In cases of non-compliance, the vehicle is included in the general population of trucks at the inspection station with no additional reporting requirements. The TTMC is responsible for ensuring that the fleet corrects any non-compliances or it will risk losing its trusted status. For Government, trusted status provided by the TTMC assures that the required state-specific data set has been evaluated.

Trusted Truck® Advantages

Advantages offered by Trusted Truck® for the fleet include providing full data-security for sensitive data via encryption and integrating driver authentication and cargo security into the system. Additionally, the server application used by the fleet can either be integrated into an existing FOC, or implemented at the TTMC as a turn-key solution to smaller fleets. Trusted Truck® also offers the possibility for fleets to go online and evaluate their compliance level with respect to industry.

Advantages offered by Trusted Truck® for the government include flexibility as inspection points can be “moved” via a geofence list upgrade to the truck and the possibility for “spot inspection” by authorities on open road. Other advantages include increasing efficiency as the population of inspection candidates is sharply reduced at the bypass point, and the option for the government to request non-required data, as allowed by the FOC.

Trusted Truck® Inspection Overview

The sequence of events during a Trusted Truck® inspection are: The vehicle enters a pre-loaded geofence, or DSRC "hotspot", triggering data collection on the vehicle. The vehicle and FOC exchange security certificates with TTMC. Vehicle-originated data is encrypted and passed to the TTMC (brake condition, etc.). Simultaneously, FOC-originated data is encrypted and passed to the TTMC (driver credentials, etc.). The TTMC then determines if trusted status is granted to the vehicle. If "trusted", the TTMC generates a bypass indicator directing the vehicle to bypass the inspection station and contacts the Government server so that the inspection station is credited with the inspection. If the TTMC determines the truck is non-compliant, the government server is not contacted and the vehicle is directed to stop at the inspection station.

The Role of the Fleet

Specific activities and responsibilities are required of the fleet in order to participate in the use of Trusted Truck®. The fleet must reference the state specific requirements -for wireless inspections- for the states in which the fleet operates. This information will be provided by the TTMC during a "new customer inquiry". The fleet is responsible to assess the expense of purchasing and installing any additional equipment, beyond manufacturer-provided sensors, needed on candidate vehicles to meet wireless inspection requirements. The fleet would also assess the benefit of increased safety scores, in terms of lower insurance costs, and time savings that will be realized with the possibility to bypass inspection stations. For the manual pre-trip conducted at the embarkation point, the fleet must require drivers to use the Wireless Inspection "Pre-Trip" function. This will detect additional out-of-compliance conditions existing on the vehicle, if it is to bypass the inspection stations on the intended route. The fleet would periodically access TTMC data features, to get a comparison on the level of compliance for the entire fleet, or even a specific vehicle, against the level of compliance for the general population of fleets monitored at the TTMC. The fleet is responsible to institute processes and take corrective actions to ensure all operating vehicles maintain compliance to the wireless inspection criteria or risk losing trusted status.

The Role of the TTMC

Specific activities and responsibilities are required of the TTMC in order to participate in the use of Trusted Truck®. The TTMC is required to maintain and enforce up-to-date criteria for wireless inspection compliance for all states and to provide timely and accurate inspection assessments for each vehicle that enters an approach zone, or when it requests self-inspection ("Pre-Trip"). The TTMC is responsible to administer the addition/deletion of geofence trigger coordinates, and provide notice to the fleet operation centers, so that they can update their vehicles with the same. These changes would occur only when a particular state has added or removed inspection stations (i.e. infrequent), or added/removed a purely virtual inspection zone. The TTMC must provide data functions, accessible online, so that fleets may compare their level of compliance with that of the general population handled by the TTMC and provide automated warnings for a fleet if their level of compliance is sufficiently below that of the general population. The TTMC must provide access to inspection authorities with regards to overall levels of compliance and enforce compliance of wireless inspection status for subscribed fleets or take remedial action to correct delinquent fleets.

The Role of the Government

Specific activities and responsibilities are required of the government in order to participate in the use of Trusted Truck®. The government needs to update the TTMC with regards to changes in wireless inspection zones, including approach zones for inspection stations, as well as virtual inspection zones. The government also needs to periodically verify the integrity of the Trusted Truck® system by performing a random "Technical Audit". During this "Technical Audit", an inspector would gain physical access to a vehicle, create a fault (e.g. dragging brake), and press the Pre-Trip button. Upon receiving the result, the inspector would then verify that the induced fault had been detected and the system is working properly. The government also needs to specify the bypass sequence required for their state. Either the TTMC will be authorized to notify the inspection station directly for each "trusted", compliant vehicle, or else the TTMC will indicate compliance directly to the government server, which would then notify the inspection station. The government needs to provide the TTMC access to government servers as needed to provide these services. Lastly, the government is responsible for crediting the inspection station for one wireless inspection, for each "trusted", compliant vehicle.

Chapter 4 – Summary and Conclusions

Lessons Learned

Phase D successfully delivered Trusted Truck® in its prototype form, giving the WRI community a service uniquely positioned to provide certain benefits, as described in the following paragraphs.

Far more inspections can be performed than would previously been possible, but the government servers will not bear the additional processing load that is required to evaluate the incoming vehicle data. In the course of an inspection, the TTMC will indeed query the government server to obtain CDL status, and driver medical status, but the bulk of the processing will occur on the TTMC servers. The benefits here are that the number of inspections can increase greatly, while the government resources are minimally taxed, and the operators bear the cost of the inspections.

Among the many benefits associated with Trusted Truck®, the most obvious "selling-point" to industry is the capability for the generally compliant fleet to avoid inspection delays. And while the vehicles equipped with wireless inspection equipment can indicate out-of-compliance items automatically, this capability is used only for their benefit. It is not used to flag vehicle non-compliance. Thus, these fleets can enjoy the benefits without enabling punitive measures due solely to adoption of the technology.

Trusted Truck® carries an additional but important built-in incentive for industry buy-in; the protection of sensitive data. Operators and OEMs protect against the access to, and collection of vehicle data that could be mined for information, and statistically analyzed to expose business patterns, and design information. The existing inspection systems are wholly government run, and have no requirement to treat data in a sensitive manner. In contrast, in the Trusted Truck® system, all data is transmitted via secure channels, and then evaluated in a closed environment. In this case, the TTMC has a real incentive to protect its customers.

The on-board system offers an opportunity for fleets to use the "Pre-Trip" feature before departing, or at any time en-route, and know if that vehicle is in compliance. While all drivers are required to perform a visual pre-trip inspection, the Trusted Truck® pre-trip feature performs an inspection automatically and thus can serve as a sanity-check for the driver. For example, while en-route, the pre-trip feature will indicate tire pressures that may have deteriorated since departure, or a cargo door that may have been tampered with at a truck-stop.

The TTMC, as a large data repository, can offer its customers the opportunity to evaluate the compliance level of their fleet with respect to an overall population of vehicles. These evaluations will be allowed such that there is no interrogation of a competing fleet. The benefit here is that a fleet can evaluate its behavior and discover trends with respect to compliance.

Given these benefits, and the fact that the concept is totally adaptable to the various WRI data-collection schemes that will be put in use in various jurisdictions, Trusted Truck® distinguishes itself as the one WRI enabler that allows the trucking industry to maintain a stake in the regulation of their own compliance.

Next Steps

It is recommended that this prototype be "scaled up" to a large field trial, to provide a more accurate picture of the ease with which the fleets can adapt to this time-saving concept, and how easily the government can adapt to the increased volume of safety inspections.

Therefore, a field trial on the order of 100 or more heavy-duty trucks operating in two or more states is recommended. This effort should include active connections with government network servers, and inspection stations. As always, the field trial will benefit from a willing, open relationship between government and industry, and serve to further realize the vision of increased safety on our nation's highways.

Appendix A - System Requirements Specification

Overview

The system shall be designed to facilitate a "wireless inspection" of a commercial vehicle as it approaches an inspection station. The concept encompasses vehicle data that can provide a profile of the vehicle that determines whether it is "trusted" enough to bypass the station or otherwise must enter the inspection station along with the general population (i.e. all other non-"trusted” trucks).

A graphical system overview is below.

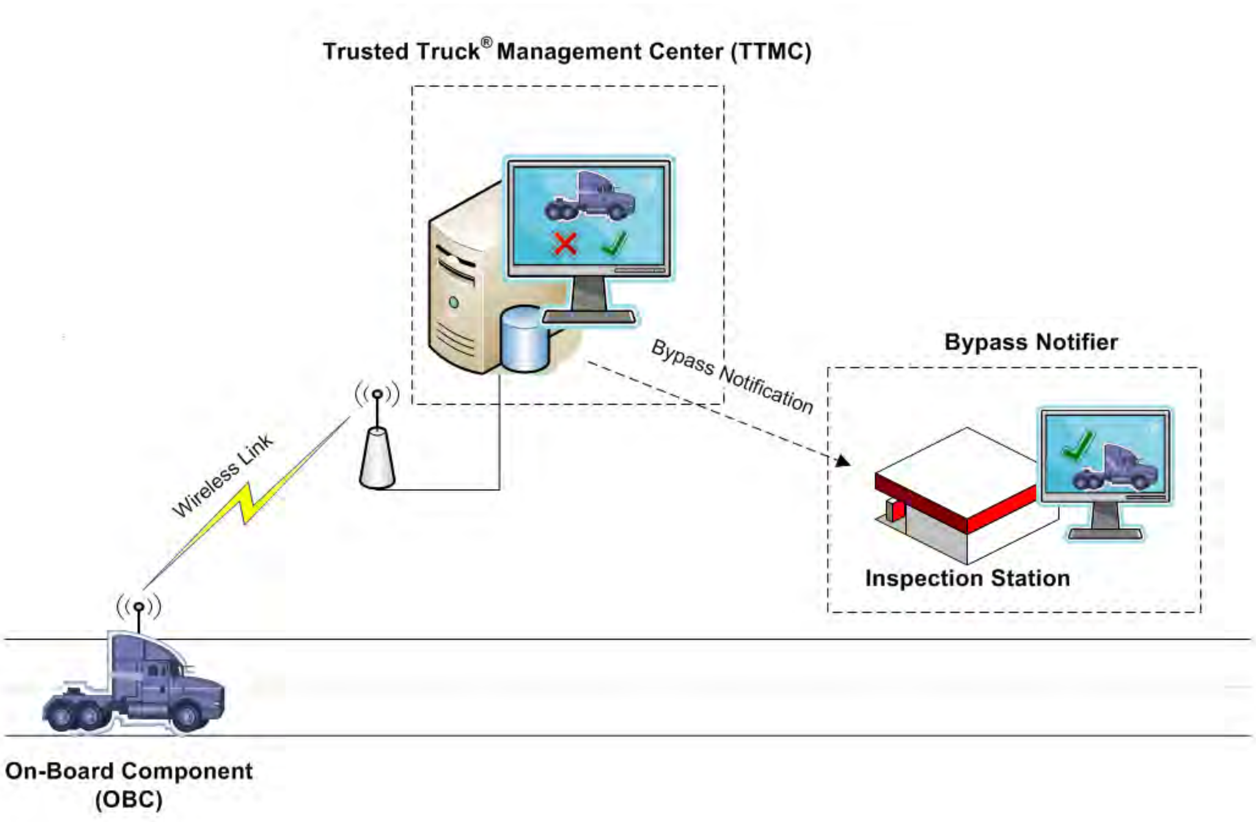


Figure 7. Diagram. System Overview

The system contains three parts, the On-Board Component (OBC), the Trusted Truck® Management Center (TTMC) and the Bypass Notifier. The On-Board Component resides in the vehicle, the TTMC resides at a (potentially) off-site location, and the Bypass Notifier resides at the inspection station. The OBC and the TTMC are communicating via a wireless communication link, while the TTMC and the Bypass Notifier use a wire link.

The TTMC will display the inspection data, received from the OBC, to the user and allow the user to respond with the approval or disapproval for bypassing the inspection station. The Bypass Notifier, when triggered by the TTMC, will provide notification to the inspection station's personnel when a “trusted” vehicle is cleared to bypass the inspection station. Additionally, the TTMC will be designed to support possible future functions that could enable historical records for each vehicle to establish "trust" in the vehicle and/or carrier with regard to inspections, leading to an incentive for vehicle operators to keep their vehicles' safety and maintenance standards high. As a further benefit, a future function of the TTMC will provide vehicle operators with notification of failed wireless inspections. This will assist vehicle operators in keeping their vehicles' safety and maintenance standards high.

On approaching the inspection station, the OBC will collect inspection data from the vehicle's electronic systems and transfer the inspection data to the TTMC. The OBC will also provide a notification to the vehicle driver regarding the approval or disapproval of bypassing the inspection station (i.e. the result of the wireless inspection), as received from the TTMC. If the vehicle must enter the inspection station, the inspection station personnel are not notified of the failed wireless inspection and the vehicle is treated no differently than the general population (i.e. all other non-"trusted” trucks).

Wireless Link

The OBC and TTMC shall communicate wirelessly via GSM according to the following diagram.

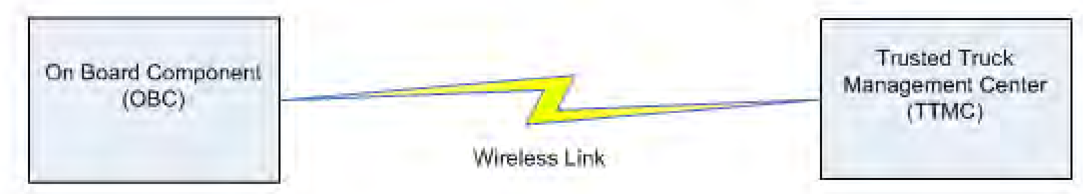


Figure 8. Diagram. Wireless Link

Sending of Inspection Data

When the vehicle approaches the inspection station, the OBC shall send vehicle and driver data to the TTMC. The approach distance at which this action is triggered shall be determined through testing in order to give ample time for the TTMC to analyze the received inspection data and respond to the vehicle, potentially allowing the vehicle to bypass the inspection station.

Vehicle Data

The OBC shall provide the following vehicle-related information to the TTMC:

- Vehicle Identification Numbers (VIN) for the tractor and trailer
- US Department of Transportation number (US DOT#)
- License plate number and issuing state abbreviation for the tractor and trailer
- International Fuel Tax Agreement (IFTA) number
- Identifying description of the tractor (color, type [daycab or sleeper] and make [Volvo])
- Identifying description of the trailer (type, color if applicable)
- Tractor tire pressure and temperature
- Trailer tire pressure and temperature
- Tractor weight
- Trailer weight
- Tractor lighting OK/NOK
- Fire extinguisher presence and operational OK/NOK
- Tractor Anti-lock Braking System OK/NOK
- Tractor brake system condition as reported by MGM's eStroke system
- Trailer brake system condition as reported by MGM's eStroke system

Driver Data

The OBC shall provide the following driver-related information to the TTMC:

- Commercial Driver’s License number (CDL#)
- Current seat belt usage

Programmable Data

The following data shall be programmable without modifying the software in the OBC:

- Vehicle Identification Numbers (VIN) for the trailer
- US Department of Transportation Number (US DOT#)
- International Fuel Tax Agreement (IFTA) number
- License plate number and issuing state abbreviation for the tractor and the trailer
- Identifying description of the tractor (color, type [daycab or sleeper] and make [Volvo])
- Identifying description of the trailer (type, color if applicable)
- Commercial Driver’s License number (CDL#)

Inspection Data Response

The TTMC shall provide approval or disapproval for bypassing the inspection station to the OBC after receiving the OBC's vehicle and driver data, giving the driver ample time to enter or bypass the inspection station. The TTMC's response may be generated manually by the user, or automatically by the TTMC.

Automatic Inspection Response Criteria

When the TTMC is configured to automatically generate inspection responses, the TTMC shall use the following criteria to determine if the vehicle is approved to bypass the inspection station.

At the instance the "wireless inspection" is performed, the vehicle shall not have:

- A driver whom is not logged-in
- One of more tires with a pressure condition reported as "extreme over pressure" or "extreme under pressure" by the vehicle's tire pressure monitoring system.
- The following conditions are allowed for any number of tires: "over pressure", "under pressure", "error indicator" and "not available".
- One or more brake assemblies reported as "non-functioning", "overstroke", or "dragging brake".
- The following condition is allowed for any number of brake assemblies: "sensor error".
- One or more brake assemblies reported as having "0% lining remaining".
- The following condition is allowed for any number of brake assemblies: "10% lining remaining".

Note: The fire extinguisher presence and operational status, tractor ABS status, and driver seal belt usage data items are not part of the automatic inspection criteria.

Driver Notification

The OBC shall notify the driver of the TTMC's approval or disapproval for bypassing the inspection station.

Inspection Data Display

The TTMC shall display the inspection data provided by a new vehicle approaching the inspection station.

Lookup of Additional Information

The TTMC shall combine the inspection data received from the vehicle with additional information as retrieved from a data store. The relationship between the received inspection data and the additional information is provided in the following table.

Table 1. Information Lookup Items

Driver’s CDL#	First and Last Name
	Residential Address
	DMV Photograph
Tractor’s USDOT#	Carrier’s Name
	Carrier’s Contact Information
	Carrier’s Logo
Tractor’s VIN	Make
	Model
	Year
	Type/Style
	Primary and Secondary (if applicable) Colors
Trailer’s VIN	Shipment – Origin Address
	Shipment – Destination Address
	Shipment – Name/Description
	Shipment – Quantity
	Shipment – Weight

Bypass Approval Notification

The TTMC shall trigger the Bypass Notifier to notify the inspection station's personnel when a "trusted” truck has been allowed to bypass the inspection station. The notification allows the bypassing truck to be positively identified and prevents needless interception by law enforcement personnel.

Bypass Disapproval Concealment

The TTMC shall not provide a notification to the inspection station's personnel when a vehicle is not approved to bypass the inspection station (i.e. fails the wireless inspection). The "untrusted" vehicle is not to be flagged or examined any differently than a vehicle of the general population.

Driver Authentication

The driver shall have successfully authenticated him/her-self with the TTMC in order to establish the vehicle as a Trusted Truck®. A vehicle without an authenticated driver shall not be “trusted”.

Data Security

All data transmitted from the OBC for use by the TTMC shall be encrypted in accordance with "Trusted Truck Crypto Document", Scott Livingston, Nov 13, 2008. This will ensure that no modification is possible by the OEM or third parties.

Guaranteed Delivery

The data transmission shall be implemented over a transport that includes guaranteed delivery (e.g. WTP, TCP).

Platform Independence

The encryption of data shall be implemented in a way to exclude any dependence on the platform hardware or software.

Transport Independence

The encryption of data shall be implemented in a way to exclude any dependence on the transport layer (e.g. UDP, TCP).

Appendix B - System Architecture Document

Architectural Description

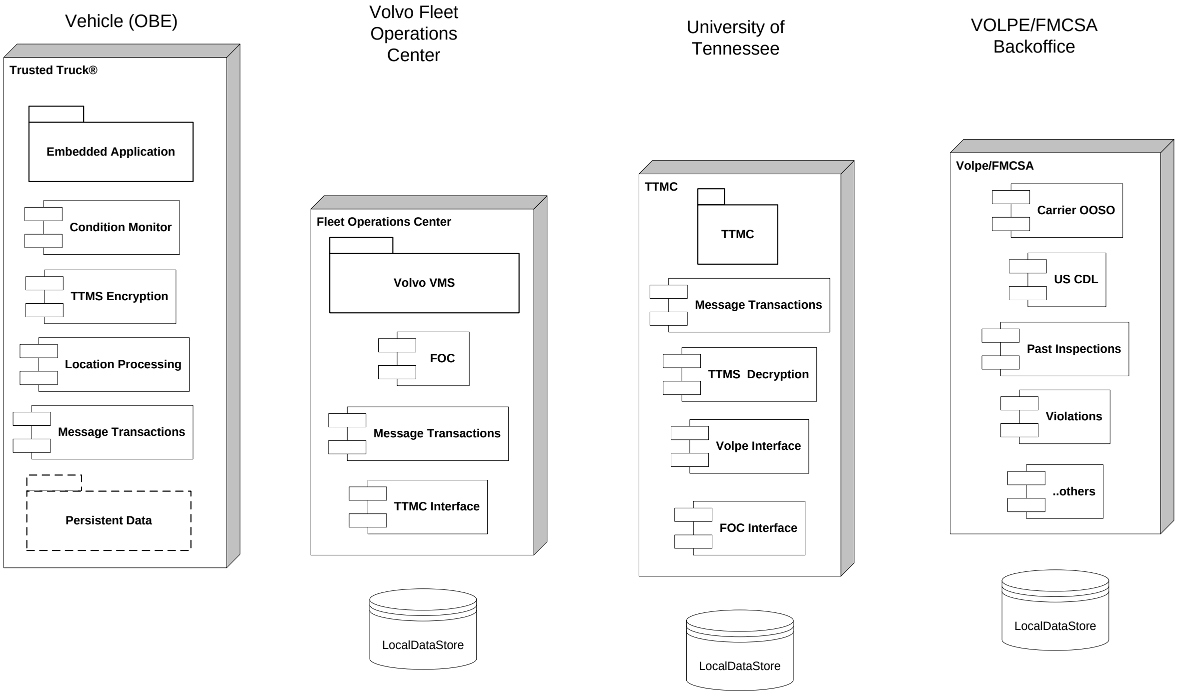


Figure 9. Diagram. Deployment View

On-Board Equipment (OBE)

OBE consists of one or many embedded applications responsible for collecting sensor and other information while the truck is deployed, keeping track of the trucks current position, and when appropriate, packaging and transmitting that information via telematic gateway to the Fleet Operations Center (FOC). These applications are specific to the original equipment manufacturer, and shall be considered proprietary from the perspective of this document. In addition, an embedded application is responsible for providing a method for entering the driver's identification, a PIN in this demonstrator package. The PIN is encapsulated into a message and transmitted for the purpose of driver identification as part of the Trusted Truck® philosophy.

The Phase C project added data encryption to the data transfer between the OBE and TTMC such that the OBE can perform encryption, but only the TTMC can perform decryption. The Phase D implementation has added an exchange of security credentials prior to transmission of the inspection message. This exchange allows the OBE and TTMC to verify the identity of the entity with which they are exchanging sensitive information. Furthermore, it allows the generation of a new encryption key by the OBE, for every inspection. Once generated, this key is used to encrypt all subsequent messages for the inspection in progress, and is discarded upon completion of the inspection. The messages that are encrypted include the inspection message that includes vehicle data items, as well as the response message from the TTMC. This provides an overall increase in the level of security, and follows the typical usage for DES encryption type message exchanges.

Fleet Operations Center (FOC)

This application is responsible for transacting data between the Volvo back office and the truck. It also provides the interface to the TTMC application being written by the University of Tennessee. This application has the responsibility of receiving an encrypted packet from the truck, adding information associated with the vehicle, driver, and payload, then transacting all the information with the TTMC, and represents the core of potential commercial services that might be offered by Volvo for fleet customers interested in taking advantage of the Trusted Truck® philosophy.

The Trusted Truck® Management Center consists of two applications: TTMC and BypassNotifier. TTMC is responsible for providing a user interface to the inspecting officer to manually decide if a truck should be "trusted", and thus be allowed to bypass the physical inspection station, or not. All inbound messages from the "trusted" truck are received by TTMC, including the TrustedTruck2Message, and the DriverAuthenticationMessage.

When a TrustedTruck2Message is received, the data is added to the internal inspection list making it available to the inspector. When an inspection has been processed, a TrustedTruck2Message is returned to the truck with Inspection Response, a Boolean value, set appropriately.

If the response was an approval to bypass, a Vehicle InspectionMessage is formatted from the data and sent to the BypassNotifier. This application is intended to display the fact that a bypass was granted thus preventing enforcement officer intervention.

Trusted Truck® Management Center (TTMC)

During the course of the Phase C project, VTEC delivered a functional TTMC application with source code and an example of an interface that could be used between FOC and TTMC. However, UT is in the process of building the TTMC at the time of this writing. It is expected to have essentially the same feature set as that demonstrated during Phase B.

Volpe/FMCSA

Some investigation was performed by VTEC relating to the nature of the data and interfaces associated with the Volpe/FMCSA systems. Volpe has implemented XML-based web services (Hall, 2004). This implies that the most likely strategy for interface with the Volpe infrastructure will be accomplished in this manner.

Data Associated with Trusted Truck®

During Phase B and C, the project aimed primarily at the SDMS (The Johns Hopkins University Applied Physics Laboratory, 2008). During Phase C, the concept of the TTMS was developed, that being the data specifically transmitted from the truck to the FOC. Work was also completed to identify additional data items that would be interesting for inclusion in the product delivered both from the FOC to the TTMC, but also from the TTMC to FMCSA.

Trusted Truck® Message Set

The information delivered from the truck in encrypted form is packaged according to the TTMS Schema as shown in Figure 12. The entire schema is defined in Figure 17.

In order to improve the marketability of the Trusted Truck® concept to FMCSA, additional information that would be of value to the government, yet not sensitive to fleets was investigated. Four items found in the CVSA inspection system, namely, the annual vehicle inspection required by FMCSA; the drivers medical card; driver skill evaluation (when available); and drug and alcohol status could be supplied with the Trusted Truck® certificate of inspection both in the prototype and by typical fleets, and thus add credibility to the certificate of inspection. The medical card information will be managed by FMCSA in 2012, further simplifying the process of delivering the information (US Department of State, 2008). For the Phase D demo, however, a medical card was included as was the FMCSA annual inspection, both delivered as “supplemental data” from the FOC to the TTMC.

Since all data may not be available from all CMV’s at once, and more data will be available in the future and added to SDMS and TTMS, it may be desirable to implement a Trusted Truck® level of inspection based loosely on the CVSA strategy, as the initiative moves forward.

Data Delivered to FMCSA – Certificate of Trust

FMCSA will receive a Certificate of Trust from the TTMC each time any given vehicle meets 100% of the inspection requirements associated with the certificate of trust. FMCSA receives nothing when a given vehicle is electronically inspected and found to be not in compliance.

Enhanced Data for FMCSA

TTMC should be prepared to deliver a number of statistical reports to FMCSA. These reports should focus on general statistics about populations of vehicles, the percentage failing the Trusted Truck® inspection, the distribution of causes of failure, etc. This type of report would be available in a multi-vehicle scenario, such as a large field trial.

Enhanced Data for Fleets

Part of the incentive for fleets to participate should be to access reports specific to their fleet. Such reports may include fleet summaries of what failures occurred on fleet trucks, how the fleet compares to the general population of Trusted Trucks®, etc. This type of report would be available in a multi-vehicle scenario, such as a large field trial.

Trusted Truck® Message Flow

The figure below details the message flow of data between the truck, the FOC, and the TTMC. An open issue is whether the TTMC must request supplementary information or if it is delivered with the encrypted report from the truck. Also, the return of the decrypted data for purposes of comparison to the fleet report from the truck is not described. These are considered to be open issues based on the completion of the TTMC by UT during the end of Phase C.

Trusted Truck® Message Flow

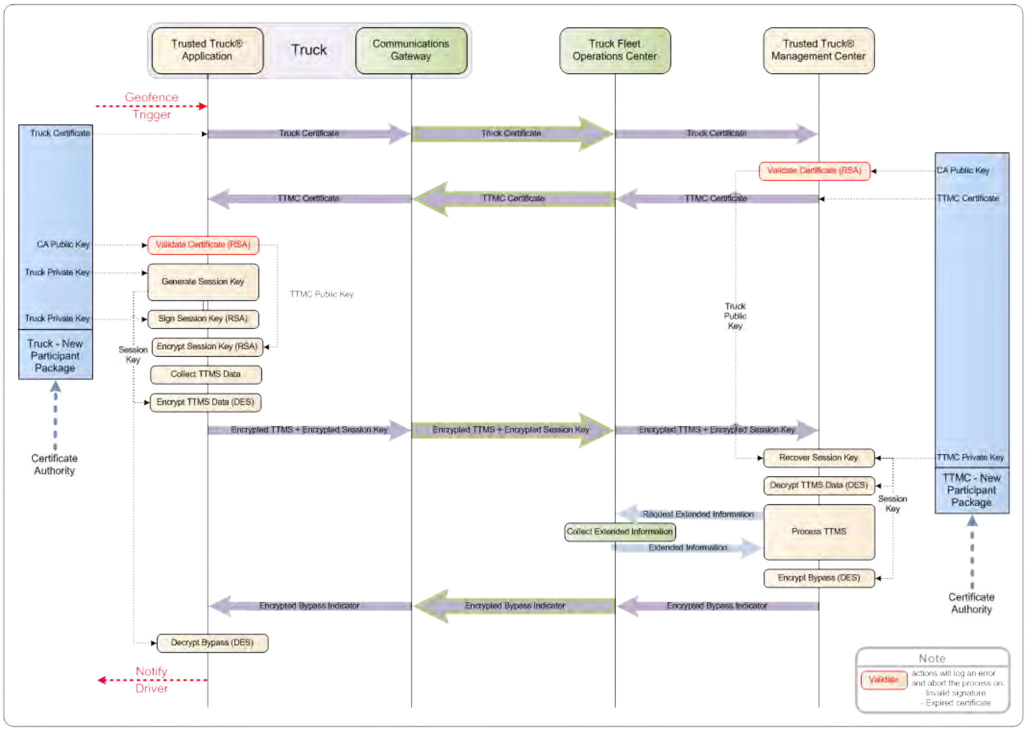


Figure 10. Diagram. Trusted Truck® Message Flow

Implementation View

VTEC.Evolution.Messages

Class BaseServiceMessage is the base class for all messages transacted through the Volvo Messaging Server, and is the only member of the package.

BaseServiceMessage
-ObsAlias : uint -ServiceId : int -ServiceVersion : int
+BaseServiceMessage() : BaseServiceMessage

Figure 11. Display. BaseServiceMessage

VTEC.Evolution.Messages.TrustedTruck2

The serialization and deserialization of this structure forms the basis of the TrustedTruck2 message. Note that BaseServiceMessage is the base class for this structure.

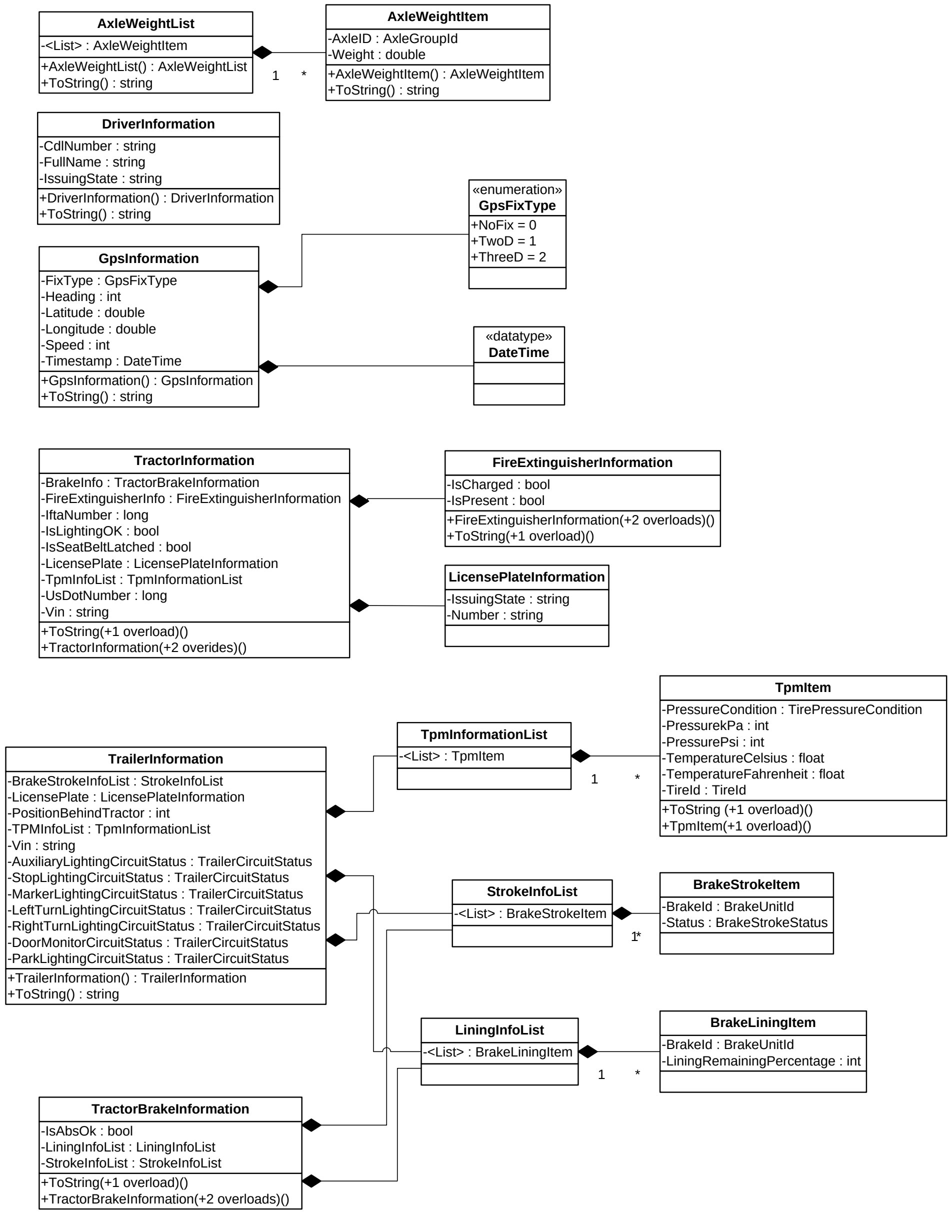

AxleWeightList
-<List> : AxleWeightItem
+AxleWeightList() : AxleWeightList
+ToString() : string
1
*
AxleWeightItem
-AxleID : AxleGroupId
-Weight : double
+AxleWeightItem() : AxleWeightItem
+ToString() : string
DriverInformation
-CdlNumber : string
-FullName : string
-IssuingState : string
+DriverInformation() : DriverInformation
+ToString() : string
«enumeration»
GpsFixType
+NoFix = 0
+TwoD = 1
+ThreeD = 2
GpsInformation
-FixType : GpsFixType
-Heading : int
-Latitude : double
-Longitude : double
-Speed : int
-Timestamp : DateTime
+GpsInformation() : GpsInformation
+ToString() : string
«datatype»
DateTime
TractorInformation
-BrakeInfo : TractorBrakeInformation
-FireExtinguisherInfo : FireExtinguisherInformation
-IftaNumber : long
-IsLightingOK : bool
-IsSeatBeltLatched : bool
-LicensePlate : LicensePlateInformation
-TpmInfoList : TpmInformationList
-UsDotNumber : long
-Vin : string
+ToString(+1 overload)()
+TractorInformation(+2 overides)()
FireExtinguisherInformation
-IsCharged : bool
-IsPresent : bool
+FireExtinguisherInformation(+2 overloads)()
+ToString(+1 overload)()
LicensePlateInformation
-IssuingState : string
-Number : string
TpmItem
-PressureCondition : TirePressureCondition
-PressurekPa : int
-PressurePsi : int
-TemperatureCelsius : float
-TemperatureFahrenheit : float
-TireId : TireId
+ToString (+1 overload)()
+TpmItem(+1 overload)()
TpmInformationList
-<List> : TpmItem
1
*
TrailerInformation
-BrakeStrokeInfoList : StrokeInfoList
-LicensePlate : LicensePlateInformation
-PositionBehindTractor : int
-TPMInfoList : TpmInformationList
-Vin : string
-AuxiliaryLightingCircuitStatus : TrailerCircuitStatus
-StopLightingCircuitStatus : TrailerCircuitStatus
-MarkerLightingCircuitStatus : TrailerCircuitStatus
-LeftTurnLightingCircuitStatus : TrailerCircuitStatus
-RightTurnLightingCircuitStatus : TrailerCircuitStatus
-DoorMonitorCircuitStatus : TrailerCircuitStatus
-ParkLightingCircuitStatus : TrailerCircuitStatus
+TrailerInformation() : TrailerInformation
+ToString() : string
StrokeInfoList
-<List> : BrakeStrokeItem
1*
BrakeStrokeItem
-BrakeId : BrakeUnitId
-Status : BrakeStrokeStatus
LiningInfoList
-<List> : BrakeLiningItem
1
*
BrakeLiningItem
-BrakeId : BrakeUnitId
-LiningRemainingPercentage : int
TractorBrakeInformation
-IsAbsOk : bool
-LiningInfoList : LiningInfoList
-StrokeInfoList : StrokeInfoList
+ToString(+1 overload)()
+TractorBrakeInformation(+2 overloads)()

Figure 12. Display. TrustedTruck2.InspectionMessage

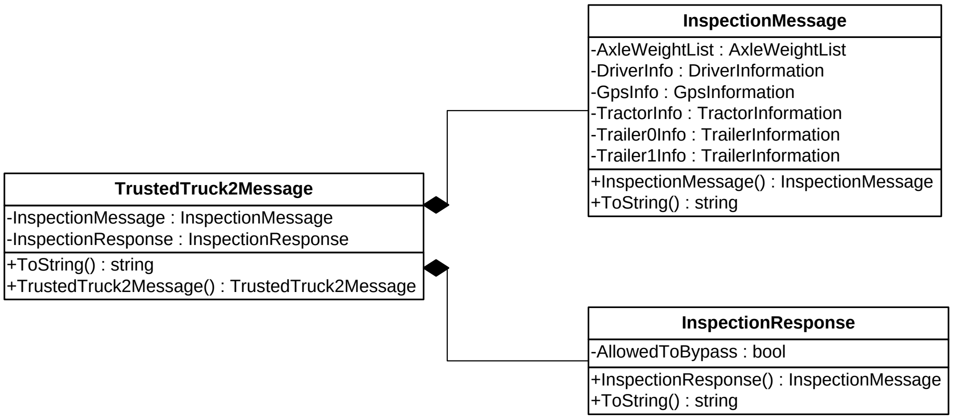

InspectionMessage
-AxleWeightList : AxleWeightList
-DriverInfo : DriverInformation
-GpsInfo : GpsInformation
-TractorInfo : TractorInformation
-Trailer0Info : TrailerInformation
-Trailer1Info : TrailerInformation
+InspectionMessage() : InspectionMessage
+ToString() : string
TrustedTruck2Message
-InspectionMessage : InspectionMessage
-InspectionResponse : InspectionResponse
+ToString() : string
+TrustedTruck2Message() : TrustedTruck2Message
InspectionResponse
-AllowedToBypass : bool
+InspectionResponse() : InspectionMessage
+ToString() : string

Figure 13. Display. TrustedTruck2Message

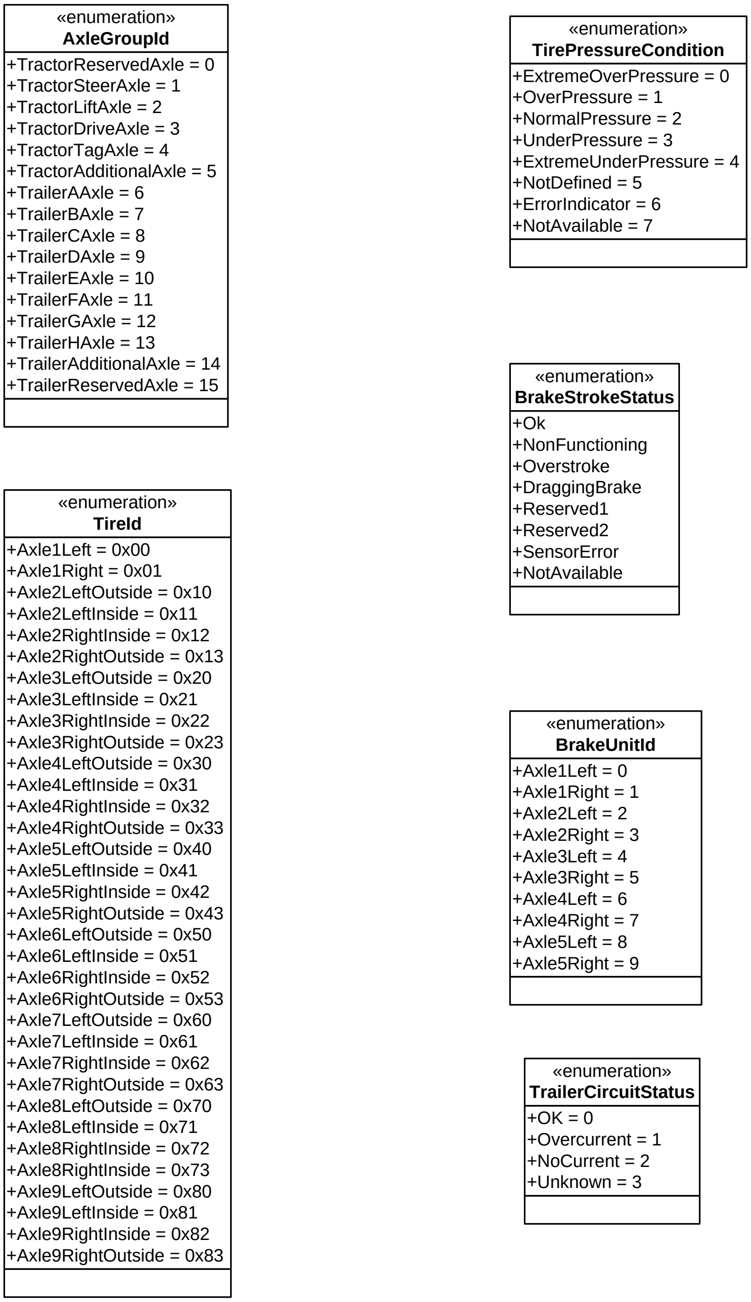
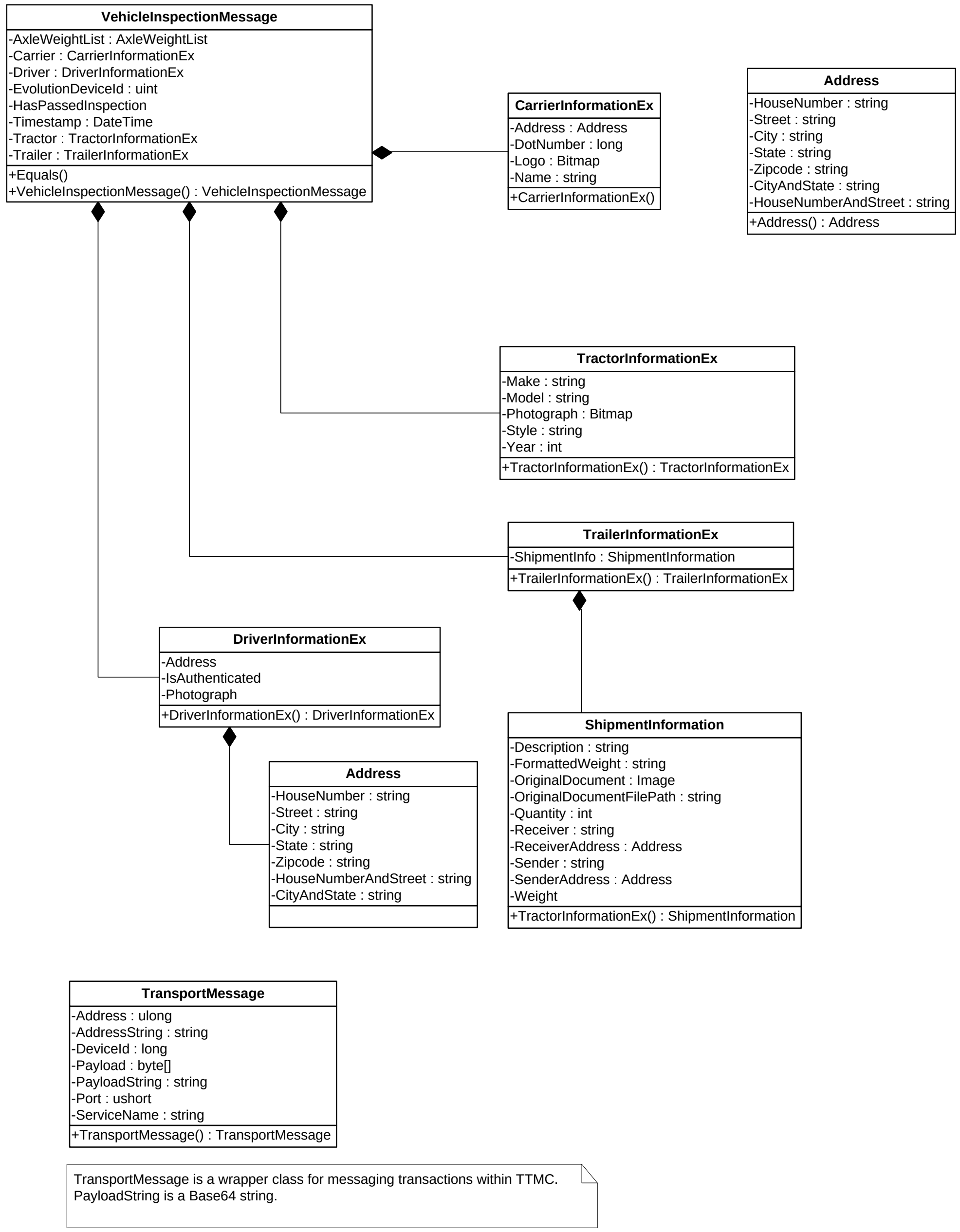


Figure 14. Display. Enumerations used within TrustedTruck2.InspectionMessage

VTEC.TrustedTruck2.BackOffice

Classes defined in this structure are the basis for messages passed within the TTMC.



TransportMessage is a wrapper class for messaging transactions within TTMC.
PayloadString is a Base64 string.

Figure 15. Display. VehicleInspectionMessage

VTEC.Evolution.Messages.DriverAuthentication

Classes defined in this structure are the basis for messages passed between TTMC and the “trusted” truck to authenticate the driver.

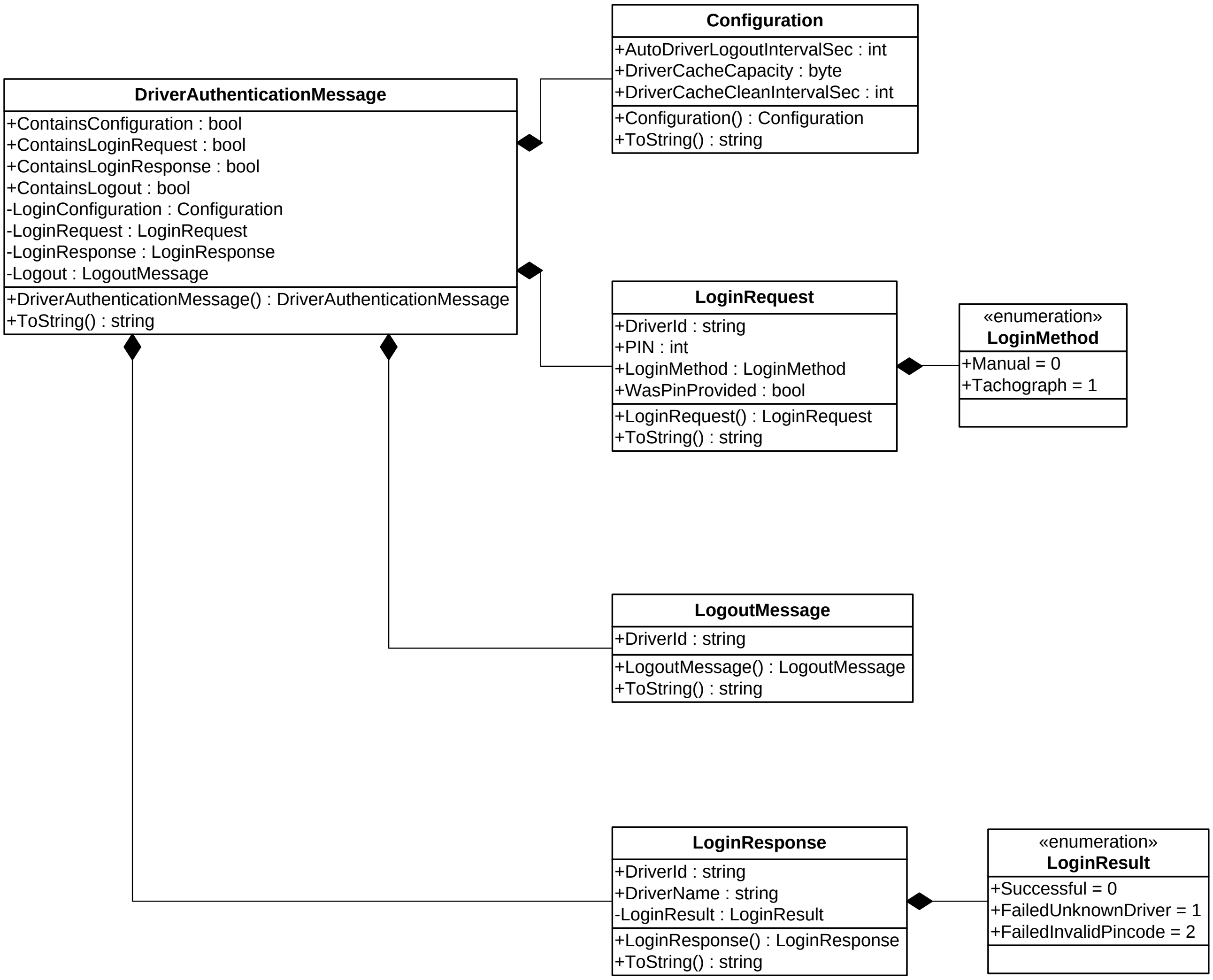

Configuration
+AutoDriverLogoutIntervalSec : int
+DriverCacheCapacity : byte
+DriverCacheCleanIntervalSec : int
+Configuration() : Configuration
+ToString() : string
DriverAuthenticationMessage
+ContainsConfiguration : bool
+ContainsLoginRequest : bool
+ContainsLoginResponse : bool
+ContainsLogout : bool
-LoginConfiguration : Configuration
-LoginRequest : LoginRequest
-LoginResponse : LoginResponse
-Logout : LogoutMessage
+DriverAuthenticationMessage() : DriverAuthenticationMessage
+ToString() : string
LoginRequest
+DriverId : string
+PIN : int
+LoginMethod : LoginMethod
+WasPinProvided : bool
+LoginRequest() : LoginRequest
+ToString() : string
«enumeration»
LoginMethod
+Manual = 0
+Tachograph = 1
LogoutMessage
+DriverId : string
+LogoutMessage() : LogoutMessage
+ToString() : string
LoginResponse
+DriverId : string
+DriverName : string
-LoginResult : LoginResult
+LoginResponse() : LoginResponse
+ToString() : string
«enumeration»
LoginResult
+Successful = 0
+FailedUnknownDriver = 1
+FailedInvalidPincode = 2

Figure 16. Display. Display. DriverAuthenticationMessage

Table 2. Correlation of Trusted Truck® to SDMS

SDMS Entity	*SDMS Data Item*	*Trusted Truck® Data Identifier*	*Data Type*	*Notes*
Carrier	USDOT number	TrustedTruck2Message.InspectionMessage.TractorInfo.UsDotNumber	long	Local FOC Data Store
Carrier	Company name	VehicleInspectionMessage.Carrier.Name	string	Local FOC Data Store
Vehicle	Tractor Vin	TrustedTruck2Message.InspectionMessage.TractorInfo.Vin	string	embedded persistent data store
Vehicle	Tractor license plate jurisdiction	TrustedTruck2Message.InspectionMessage.TractorInfo.LicensePlate.IssuingState	string	Local FOC Data Store
Vehicle	Tractor license plate ID	TrustedTruck2Message.InspectionMessage.TractorInfo.LicensePlate.Number	string	Local FOC Data Store
Vehicle	Tractor unit number	Not Available		
Vehicle	Brakes, Tractor	TrustedTruck2Message.InspectionMessage.TractorInfo.BrakeInfo	TractorBrakeInformation	on-board sensor
Vehicle	Brakes, Trailer 1	TrustedTruck2Message.InspectionMessage.Trailer0Info.BrakeStrokeInfoList	TrailerInformation	on-board sensor
Vehicle	Brakes, Trailer 2	TrustedTruck2Message.InspectionMessage.Trailer1Info.BrakeStrokeInfoList	TrailerInformation	on-board sensor
Vehicle	Tire pressure, Tractor	TrustedTruck2Message.InspectionMessage.TractorInfo.TpmInfoList	TractorBrakeInformation	on-board sensor
Vehicle	Tire pressure, Trailer 0	TrustedTruck2Message.InspectionMessage.Trailer0Info.TpmInfoList	TrailerInformation	on-board sensor
Vehicle	Tire pressure, Trailer 1	TrustedTruck2Message.InspectionMessage.Trailer1Info.TpmInfoList	TrailerInformation	on-board sensor
Vehicle	Vehicle location	TrustedTruck2Message.InspectionMessage.GpsInfo	GpsInformation	Satellite communication
Vehicle	Weight	TrustedTruck2Message.InspectionMessage.AxleWeightList	AxleWeightList	on-board sensor
Vehicle	Date	TrustedTruck2Message.InspectionMessage.GpsInfo.Timestamp	DateTime	on-board sensor
Vehicle	Time	TrustedTruck2Message.InspectionMessage.GpsInfo.Timestamp	DateTime	on-board sensor
Vehicle Status	Lighting	TrustedTruck2Message.InspectionMessage.TractorInfo.isLightingOK	Boolean	on-board sensor
Vehicle Status	Safety belt	TrustedTruck2Message.InspectionMessage.TractorInfo.isSeatBeltLatched	Boolean	on-board sensor
Driver	Jurisdiction	TrustedTruck2Message.InspectionMessage.DriverInfo.IssuingState	string	Local FOC Data Store
Driver	License ID	TrustedTruck2Message.InspectionMessage.DriverInfo..CdlNumber	string	Local FOC Data Store
Driver	First name	TrustedTruck2Message.InspectionMessage.DriverInfo.FullName	string	Local FOC Data Store
Driver	Last name	TrustedTruck2Message.InspectionMessage.DriverInfo.FullName	string	Local FOC Data Store
Driver	PIN/ID	VehicleInspectionMessage.Driver.isAuthenticated	Boolean	PIN number is not available
Driver Co-driver	Jurisdiction	Not Available		
Driver Co-driver	License ID	Not Available		
Driver Co-driver	First name	Not Available		
Driver Co-driver	Last name	Not Available		
Driver Co-driver	PIN/ID	Not Available		
Driver Log event data	Sequence ID	Not Available		
Driver Log event data	Status code	Not Available		
Driver Log event data	Date	Not Available		
Driver Log event data	Time	Not Available		

SDMS Entity	***SDMS Data Item***	***Trusted Truck® Data Identifier***	***Data Type***	***Notes***
Driver Log event data	Latitude	Not Available		
Driver Log event data	Longitude	Not Available		
Driver Log event data	Place name	Not Available		
Driver Log event data	Place distance	Not Available		
Driver Log event data	Total vehicle miles	Not Available		
Driver Log event data	Event update status code	Not Available		
Driver Log event data	status code	Not Available		
Driver Log event data	Error code	Not Available		
Driver Log event data	Update date	Not Available		
Driver Log event data	Update time	Not Available		
Driver Log event data	Update person ID	Not Available		
Driver Log event data	Update text	Not Available		
Driver Log data	24-hour period start time	Not Available		
Driver Log data	Multiday basis used	Not Available		
Equipment Identifier	Equipment ID (e.g., trailer unit #0)	TrustedTruck2Message.InspectionMessage.Trailer0Info.Vin	string	Local FOC Data Store
Equipment Identifier	Equipment ID (e.g., trailer unit #1)	TrustedTruck2Message.InspectionMessage.Trailer1Info.Vin	string	Local FOC Data Store
Equipment Identifier	Equipment license plate jurisdiction, trailer unit #0	TrustedTruck2Message.InspectionMessage.Trailer0Info.LicensePlate.IssuingState	string	Local FOCC Data Store
Equipment Identifier	Equipment license plate jurisdiction, trailer unit # 1	TrustedTruck2Message.InspectionMessage.Trailer1Info.LicensePlate.IssuingState	string	Local FOC Data Store
Equipment Identifier	Equipment license plate ID, trailer unit #0	TrustedTruck2Message.InspectionMessage.Trailer0Info.LicensePlate.IssuingState	string	Local FOC Data Store
Equipment Identifier	Equipment license plate ID, trailer unit #1	TrustedTruck2Message.InspectionMessage.Trailer1Info.LicensePlate.IssuingState	string	Local FOC Data Store
Shipment Identifier	Shipping document number	VehicleInspectionMessage.Trailer.ShipmentInformation.OriginalDocument	Image	Local FOCC Data Store
Encounter Date/time	MM/DD/YYYY	Not Available		
Encounter Date/time	HH:MM:SS	Not Available		
Encounter Location	Latitude	Not Available		
Encounter Location	Longitude	Not Available		
Encounter Location	Encounter ID	Not Available		
Encounter Location	Triggering event	Not Available		
Transponder Identifier	Serial Number	VehicleInspectionMessage.EvolutionDeviceId		embedded persistent data store

CVSA Inspections

It is assumed that CVSA will issue a new level of inspection to define wireless roadside inspection (WRI). Currently, CVSA defines five levels of inspection as follows:

Table 3. CVSA Inspections.

Item	Description	Level I	Level II	Level III	Level IV	Level V
1	Drivers' License	✓	✓	✓		
2	Medical Examiner's Certificate and Skill Performance Evaluation (SPE) Certificate (if applicable)	✓	✓	✓		
3	Alcohol and Drugs	✓	✓	✓		
4	Drivers' Log (Hours-of-Service and Duty Status)	✓	✓	✓		
5	Seatbelt System	✓	✓	✓		✓
6	Vehicle Inspection Report	✓	✓	✓		✓
7	Brake Systems	✓	✓			✓
8*	Coupling Devices	✓	✓			✓
9*	Exhaust Systems	✓	✓			✓
10*	Frame	✓	✓			✓
11*	Fuel Systems	✓	✓			✓
12	Lighting Devices (Brake, Head, and Tail Lamps, Turn Signals, Lamps on Projecting Loads)	✓	✓			✓
13*	Safe Loading	✓	✓			✓
14*	Steering Mechanism	✓	✓			✓
15*	Suspension	✓	✓			✓
16	Tires	✓	✓			✓
17*	Van and Open Top Trailer Bodies	✓	✓			✓
18*	Wheels, Rims, and Hubs	✓	✓			✓
19*	Windshield Wipers	✓	✓			✓
20*	Emergency Exits (for busses)	✓	✓			✓
21	Hazardous Materials Requirements (if applicable)	✓		✓		✓
22	One time special inspection of a particular item				✓	
23	CVSA decal issued for "Pass Inspection" (No Violations/defects found in items 7-21)	✓				

* denotes items that cannot be inspected electronically.

Trusted Truck® Message Set Schema

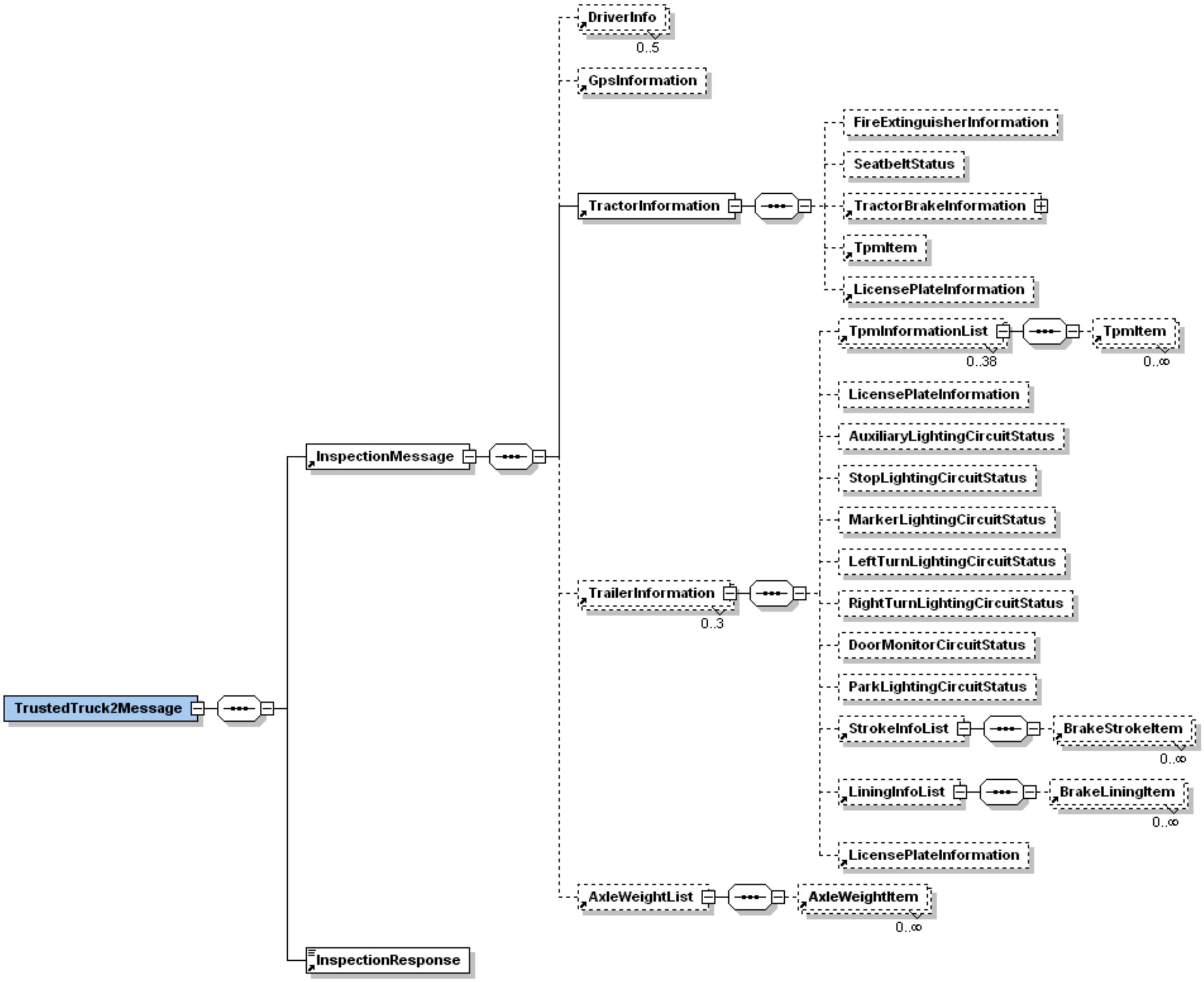


Figure 17. Display. Trusted Truck® Message Set Schema

Full Schema View

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XML Spy v4.4 U (http://www.xmlspy.com) by Emily C. Williams (Volvo Technology  of America) -->
<!--W3C Schema generated by XML Spy v4.4 U (http://www.xmlspy.com)-->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
        <xs:simpleType name="TireId">
                <xs:restriction base="xs:string">
                        <xs:enumeration value="Axle1Left"/>
                        <xs:enumeration value="Axle1Right"/>
                        <xs:enumeration value="Axle2LeftOutside"/>
                        <xs:enumeration value="Axle2LeftInside"/>
                        <xs:enumeration value="Axle2RightInside"/>
                        <xs:enumeration value="Axle2RightOutside"/>
                        <xs:enumeration value="Axle3LeftOutside"/>
                        <xs:enumeration value="Axle3LeftInside"/>
                        <xs:enumeration value="Axle3RightInside"/>
                        <xs:enumeration value="Axle3RightOutside"/>
                        <xs:enumeration value="Axle4LeftOutside"/>
                        <xs:enumeration value="Axle4LeftInside"/>
                        <xs:enumeration value="Axle4RightInside"/>
                        <xs:enumeration value="Axle4RightOutside"/>
                        <xs:enumeration value="Axle5LeftOutside"/>
                        <xs:enumeration value="Axle5LeftInside"/>
                        <xs:enumeration value="Axle5RightInside"/>
                        <xs:enumeration value="Axle5RightOutside"/>
                        <xs:enumeration value="Axle6LeftOutside"/>
                        <xs:enumeration value="Axle6LeftInside"/>
                        <xs:enumeration value="Axle6RightInside"/>
                        <xs:enumeration value="Axle6RightOutside"/>
                        <xs:enumeration value="Axle7LeftOutside"/>
                        <xs:enumeration value="Axle7LeftInside"/>
                        <xs:enumeration value="Axle7RightInside"/>
                        <xs:enumeration value="Axle7RightOutside"/>
                        <xs:enumeration value="Axle8LeftOutside"/>
                        <xs:enumeration value="Axle8LeftInside"/>
                        <xs:enumeration value="Axle8RightInside"/>
                        <xs:enumeration value="Axle8RightOutside"/>
                        <xs:enumeration value="Axle9LeftOutside"/>
                        <xs:enumeration value="Axle9LeftInside"/>
                        <xs:enumeration value="Axle9RightInside"/>
                        <xs:enumeration value="Axle9RightOutside"/>
                </xs:restriction>
        </xs:simpleType>
        <xs:simpleType name="AxleGroupId">
                <xs:restriction base="xs:string">
                        <xs:enumeration value="TractorReservedAxle"/>
                        <xs:enumeration value="TractorSteerAxle"/>
                        <xs:enumeration value="TractorLiftAxle"/>
                        <xs:enumeration value="TractorDriveAxle"/>
                        <xs:enumeration value="TractorTagAxle"/>
                        <xs:enumeration value="TractorAdditionalAxle"/>
                        <xs:enumeration value="TrailerAAxle"/>
                        <xs:enumeration value="TrailerBAxle"/>
                        <xs:enumeration value="TrailerCAxle"/>
                        <xs:enumeration value="TrailerDAxle"/>
                        <xs:enumeration value="TrailerEAxle"/>
                        <xs:enumeration value="TrailerFAxle"/>
                        <xs:enumeration value="TrailerGAxle"/>
                        <xs:enumeration value="TrailerHAxle"/>
                        <xs:enumeration value="TrailerAdditionalAxle"/>
                        <xs:enumeration value="TrailerReservedAxle"/>
                </xs:restriction>
        </xs:simpleType>
        <xs:simpleType name="TirePressureCondition">
                <xs:restriction base="xs:string">
                        <xs:enumeration value="ExtremeOverPressure"/>
                        <xs:enumeration value="OverPressure"/>
                        <xs:enumeration value="NormalPressure"/>
                        <xs:enumeration value="UnderPressure"/>
                        <xs:enumeration value="ExtremeUnderPressure"/>
                        <xs:enumeration value="NotDefined"/>
                        <xs:enumeration value="ErrorIndicator"/>
                        <xs:enumeration value="NotAvailable"/>
                </xs:restriction>
        </xs:simpleType>
        <xs:simpleType name="BrakeStrokeStatus">
                <xs:restriction base="xs:string">
                        <xs:enumeration value="Ok"/>
                        <xs:enumeration value="NonFunctioning"/>
                        <xs:enumeration value="Overstroke"/>
                        <xs:enumeration value="DragglingBrake"/>
                        <xs:enumeration value="Reserved1"/>
                        <xs:enumeration value="Reserved2"/>
                        <xs:enumeration value="SensorError"/>
                        <xs:enumeration value="NotAvailable"/>
                </xs:restriction>
        </xs:simpleType>
        <xs:simpleType name="BrakeUnitID">
                <xs:restriction base="xs:string">
                        <xs:enumeration value="Axle1Left"/>
                        <xs:enumeration value="Axle1Right"/>
                        <xs:enumeration value="Axle2Left"/>
                        <xs:enumeration value="Axle2Right"/>
                        <xs:enumeration value="Axle3Left"/>
                        <xs:enumeration value="Axle3Right"/>
                        <xs:enumeration value="Axle4Left"/>
                        <xs:enumeration value="Axle4Right"/>
                        <xs:enumeration value="Axle5Left"/>
                        <xs:enumeration value="Axle5Right"/>
                </xs:restriction>
        </xs:simpleType>
        <xs:simpleType name="GpsFixType">
                <xs:restriction base="xs:string">
                        <xs:enumeration value="NoFix"/>
                        <xs:enumeration value="TwoD"/>
                        <xs:enumeration value="ThreeD"/>
                </xs:restriction>
        </xs:simpleType>
        <xs:simpleType name="TrailerCircuitStatus">
                <xs:restriction base="xs:string">
        <xs:enumeration value="OK"/>
        <xs:enumeration value="Overcurrent"/>
        <xs:enumeration value="NoCurrent"/>
        <xs:enumeration value="Unknown"/>
    </xs:restriction>
</xs:simpleType>
<xs:element name="AxleWeightItem" nillable="true">
    <xs:complexType>
        <xs:attribute name="AxleID" type="AxleGroupId" use="optional"/>
        <xs:attribute name="Weight" type="xs:double" use="optional"/>
    </xs:complexType>
</xs:element>
<xs:element name="AxleWeightList" nillable="true">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="AxleWeightItem" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="DriverInfo">
    <xs:complexType>
        <xs:attribute name="CdlNumber" type="xs:string" use="optional"/>
        <xs:attribute name="FullName" type="xs:string" use="optional"/>
        <xs:attribute name="IssuingState" type="xs:string" use="optional"/>
    </xs:complexType>
</xs:element>
<xs:element name="GpsInformation" nillable="true">
    <xs:complexType>
        <xs:attribute name="FixType" type="GpsFixType" use="optional"/>
        <xs:attribute name="Heading" type="xs:int" use="optional"/>
        <xs:attribute name="Latitude" type="xs:double" use="optional"/>
        <xs:attribute name="Longitude" type="xs:double" use="optional"/>
        <xs:attribute name="Speed" type="xs:int" use="optional"/>
        <xs:attribute name="Timestamp" type="xs:dateTime" use="optional"/>
    </xs:complexType>
</xs:element>
<xs:element name="InspectionMessage">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="DriverInfo" minOccurs="0" maxOccurs="5"/>
            <xs:element ref="GpsInformation" minOccurs="0"/>
            <xs:element ref="TractorInformation"/>
            <xs:element ref="TrailerInformation" minOccurs="0" maxOccurs="3"/>
            <xs:element ref="AxleWeightList" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="InspectionResponse" type="xs:boolean"/>
<xs:element name="TractorInformation">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="FireExtinguisherInformation" minOccurs="0">
                <xs:complexType>
                    <xs:attribute name="IsCharged" type="xs:boolean" use="optional"/>
                    <xs:attribute name="IsPresent" type="xs:boolean" use="optional"/>
                </xs:complexType>
            </xs:element>
            <xs:element name="SeatbeltStatus" minOccurs="0">
                <xs:complexType>
                    <xs:attribute name="IsLatched" type="xs:boolean" use="optional"/>
                </xs:complexType>
            </xs:element>
            <xs:element ref="TractorBrakeInformation" minOccurs="0"/>
            <xs:element ref="TpmItem" minOccurs="0"/>
            <xs:element ref="LicensePlateInformation" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="isLightingOK" type="xs:boolean" use="optional"/>
        <xs:attribute name="IftaNumber" type="xs:string" use="optional"/>
        <xs:attribute name="USDotNumber" type="xs:long" use="optional"/>
        <xs:attribute name="VIN" type="xs:string" use="optional"/>
    </xs:complexType>
</xs:element>
<xs:element name="TrailerInformation">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="TpmInformationList" minOccurs="0" maxOccurs="38"/>
            <xs:element name="LicensePlateInformation" nillable="true" minOccurs="0">
                <xs:complexType>
                    <xs:attribute name="IssuingState" type="xs:string" use="optional"/>
                    <xs:attribute name="Number" type="xs:string" use="optional"/>
                </xs:complexType>
            </xs:element>
            <xs:element name="AuxiliaryLightingCircuitStatus" nillable="true" minOccurs="0">
                <xs:complexType>
                    <xs:attribute name="AuxiliaryLightingCircuitStatus" type="TrailerCircuitStatus" use="optional"/>
                </xs:complexType>
            </xs:element>
            <xs:element name="StopLightingCircuitStatus" nillable="true" minOccurs="0">
                <xs:complexType>
                    <xs:attribute name="StopLightingCircuitStatus" type="TrailerCircuitStatus" use="optional"/>
                </xs:complexType>
            </xs:element>
            <xs:element name="MarkerLightingCircuitStatus" nillable="true" minOccurs="0">
                <xs:complexType>
                    <xs:attribute name="MarkerLightingCircuitStatus" type="TrailerCircuitStatus" use="optional"/>
                </xs:complexType>
            </xs:element>
            <xs:element name="LeftTurnLightingCircuitStatus" nillable="true" minOccurs="0">
                <xs:complexType>
                    <xs:attribute name="LeftTurnLightingCircuitStatus" type="TrailerCircuitStatus" use="optional"/>
                </xs:complexType>
            </xs:element>
            <xs:element name="RightTurnLightingCircuitStatus" nillable="true" minOccurs="0">
                <xs:complexType>
                    <xs:attribute name="RightTurnLightingCircuitStatus" type="TrailerCircuitStatus" use="optional"/>
                </xs:complexType>
            </xs:element>
            <xs:element name="DoorMonitorCircuitStatus" nillable="true" minOccurs="0">
                <xs:complexType>
                    <xs:attribute name="DoorMonitorCircuitStatus" type="TrailerCircuitStatus" use="optional"/>
                </xs:complexType>
            </xs:element>
```

```
                <xs:element name="ParkLightingCircuitStatus" nillable="true" minOccurs="0">
                    <xs:complexType>
                        <xs:attribute name="ParkLightingCircuitStatus" type="TrailerCircuitStatus" use="optional"/>
                    </xs:complexType>
                </xs:element>
                <xs:element ref="StrokeInfoList" minOccurs="0"/>
                <xs:element ref="LiningInfoList" minOccurs="0"/>
                <xs:element ref="LicensePlateInformation" minOccurs="0"/>
            </xs:sequence>
            <xs:attribute name="VIN" type="xs:string" use="optional"/>
            <xs:attribute name="PositionBehindTractor" type="xs:int" use="optional"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="TrustedTruck2Message">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="InspectionMessage"/>
                <xs:element ref="InspectionResponse"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="TpmItem" nillable="true">
        <xs:complexType>
            <xs:attribute name="PressureCondition" type="TirePressureCondition" use="optional"/>
            <xs:attribute name="PressurekPa" type="xs:int" use="optional"/>
            <xs:attribute name="PressurePsi" type="xs:int" use="optional"/>
            <xs:attribute name="TemperatureCelsius" type="xs:float" use="optional"/>
            <xs:attribute name="TemperatureFahrenheit" type="xs:float" use="optional"/>
            <xs:attribute name="TireId" type="TireId" use="optional"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="TractorBrakeInformation">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="BrakeLiningItem" minOccurs="0" maxOccurs="10"/>
                <xs:element ref="BrakeStrokeItem" minOccurs="0" maxOccurs="10"/>
            </xs:sequence>
            <xs:attribute name="IsAbsOk" type="xs:boolean" use="optional"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="BrakeLiningItem" nillable="true">
        <xs:complexType>
            <xs:attribute name="BrakeId" type="BrakeUnitID" use="optional"/>
            <xs:attribute name="LiningRemainingPercentage" type="xs:float" use="optional"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="BrakeStrokeItem" nillable="true">
        <xs:complexType>
            <xs:attribute name="BrakeId" type="BrakeUnitID" use="optional"/>
            <xs:attribute name="BrakeStrokeStatus" type="BrakeStrokeStatus" use="optional"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="TpmInformationList" nillable="true">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="TpmItem" minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="LicensePlateInformation" nillable="true">
        <xs:complexType>
            <xs:attribute name="IssuingState" type="xs:string" use="optional"/>
            <xs:attribute name="Number" type="xs:string" use="optional"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="FireExtinguisherInformation">
        <xs:complexType>
            <xs:attribute name="IsCharged" type="xs:boolean" use="optional"/>
            <xs:attribute name="IsPresent" type="xs:boolean" use="optional"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="LiningInfoList" nillable="true">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="BrakeLiningItem" minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="StrokeInfoList" nillable="true">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="BrakeStrokeItem" minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

References

Hall J., 2004. Web Services open the door to FMCSA safety data. Retrieved June 1, 2009 from www.atsip.org/oldsite/forum2004/Sessions/Wednesday_25-36/S34/s34_JeffHall_FMCSAWebServices.ppt

US Department of State: FMCSA Improves Medical Requirements for Commercial Truck and Bus Drivers. (2 December, 2008). *M2 Presswire*. Retrieved June 1, 2009, from ProQuest Computing database. (Document ID: 1604895011).

The Johns Hopkins University Applied Physics Laboratory, 2008. Concept of Operations (ConOps) for Wireless Roadside Inspection. *Federal Motor Carrier Safety Administration*. Document ID: NSTD-07-0104 D.5.

Appendix C – “A Data Security Protocol for the Trusted Truck® System”

A Data Security Protocol for the Trusted Truck® System

S. A. Bulusu, B. Arazi, I. Arel, A. Davis
EECS Department
University of Tennessee
{sbulusu,barazi,itamar}@utk.edu

G. Bitar
Volvo Technologies
Greensboro, NC
george.bitar@volvo.com

ABSTRACT

Security has become one of the major concerns in the context of Intelligent Transportation Systems (ITS). The Trusted Truck® system provides an efficient wireless communication mechanism for safe exchange of messages between moving vehicles (trucks) and roadside inspection stations. Vehicles and station are equipped with processing units but with different computational capabilities. To render data exchange in Trusted Truck® more secure, this paper proposes a secured data protocol which ensures data integrity, message authentication and non-repudiation. The uniqueness of the protocol is that it effectively exploits the asymmetry of computational resources. It is cost-effective, resource-efficient and is embedded within the Trusted Truck® environment without demanding any additional hardware infrastructure. The protocol balances the computational load between vehicles and stations by incorporating an innovative key transport mechanism. Digital signatures and encryption techniques are utilized for authentication and data confidentiality. Cryptography algorithms along with optimization methods are used for digital signatures. The execution time of the algorithms is analyzed along with clear demonstration of the benefits offered by the proposed scheme.

Categories and Subject Descriptors

D.4.5 [**Security and Protection**]: Cryptographic Controls

General Terms

Algorithms, Performance, Security

Keywords

Trusted Truck® system, secured data protocol, public-key cryptography, key-transport mechanism

1. INTRODUCTION

The US Department of Transportation takes the responsibility to ensure that heavy vehicle carriers are complying with the safety regulations without affecting the time and profitability of these carriers. Intelligent Transportation Systems (ITS) utilize modern technologies and systems in an aim to improve a broad range of transportation systems. The Trusted Truck® project is one such project which allowed the US DOT to significantly shorten carrier verification times by providing a wireless communication link to verify the credentials of vehicles while adhering to ITS standards.

The Trusted Truck® Program was initiated in 2003 as a joint effort by Volvo Group North America, the National Transportation Research Centre, Inc., (NTRCI), and The University of Tennessee. The primary vision behind this effort is to provide safe and efficient heavy vehicle transportation. One technology that provides a quantum leap in the percentage of vehicles inspected is wireless vehicle inspection. This in turn will enable far greater levels of highway safety, and provide improvements in homeland security. But any wireless vehicle inspection system that allows the unsecured transmission of vehicle data will be rejected by the private sector, creating a legislative roadblock that will take years to resolve. The data security techniques discussed here, are critical for a practical widespread implementation that will allow industry acceptance for this system.

The Trusted Truck® system will make it possible for government to reduce the population of potential violators to a degree never before possible. The system will also make it possible for trucking businesses to prove compliance, and thus reduce the risk of losing significant amounts of time waiting for manual inspections. These two benefits are critical to the acceptance of the Trusted Truck® system by government and industry alike.

Of particular focus is the ability to present and verify credentials, as well as encrypt/decrypt the vehicle inspection payload in a limited time-window bounded by the vehicle's approach to the inspection station. This is where efficiency gains are realized by using a data security technique that is tailored for this implementation. Equally important is the ability to carry out these computations within the bounds of the processing power available on the vehicles typical to the long-haul truck industry. Also important is the fact that certificate installation on vehicles can be carried out through an existing channel, namely the manufacturer's software download procedure that is heavily safe-guarded, as it protects the liability of vehicle safety systems and valuable intellectual property. These requirements have all been satisfied by the Trusted Truck® system.

2. SECURITY REQUIREMENTS

Information security forms an important aspect of secured wireless communication between vehicles and road side inspection stations. Regardless of who is involved, all parties in any transaction must have confidence that certain information security objectives have been met. For decades, cryptographic techniques have been in employed in order to provide information security and/or secured communication. Modern cryptography can be divided into two classes: symmetric key cryptography and

Conference'04, Month 1–2, 2004, City, State, Country.

public key cryptography. The former uses the same key for encryption and decryption whereas the latter uses two different keys: one public and the other private. RSA is a public key cryptographic method which has been successfully used for over 20 years in secured message transfers [2][4]. RSA uses a pair of keys for encryption and decryption as well as for digital signatures [5]. Digital signatures are used to verify the authenticity of a particular sender [4]. In most secured communications, RSA is employed for digitally signing and transferring a secret (session) key which is utilized to encrypt messages exchanged by the communicating parties. Upon successful verification of the authenticity of a sender, the secret key is extracted and messages can be encrypted and decrypted.

For the Trusted Truck® system to be secure, a data security infrastructure should be in place such that messages are exchanged only between trusted parties. The necessity for a robust data security infrastructure for such a system initiated the development of a resource-efficient data protocol for the exchange of messages between the vehicles (trucks) and inspection stations. In an environment where critical information is exchanged between the vehicles and the stations, there is always a threat of data manipulation, tampering of vehicle sensors, and inappropriate identification of the participants. This paper presents a cost-effective and resource-efficient secured data protocol which has been customized to the Trusted Truck® environment in an effort to provide data confidentiality and message authentication. The paper also introduces an innovative way to use and enhance the speed of an existing asymmetric key cryptographic algorithm to balance the computational load between the vehicle and the road side inspection station. The designed protocol utilizes RSA for the digital signatures and DES [3] for encryption and decryption. The DES key is transported safely through a key-transport mechanism using RSA. Mathematical explanations of the algorithms are provided to support the observed performance improvements.

1. SYSTEM DESCRIPTION

1.1 Communications Framework

The Trusted Truck® system involves three main entities - vehicles (trucks), station (departing station, weigh station, arriving station) and a Certificate Authority (CA). The departing station is the point at which the vehicle's trip begins, the weigh stations are the inspection stations along the highway and the arriving station denotes the final destination of the vehicle. In addition to these there is driver and cargo information which is crucial in the context of vehicle identification at the departing stations. It is important to note that none of the exchanged messages in this model are encrypted. To make this system more secure and protect messages from adversarial interference, a secured protocol is designed which does not modify the structure of the existing system, but rather revises the manner by which messages are exchanged. The protocol is designed such that the identification and authentication mechanisms are embedded in the messages exchanged between the vehicles and stations.

1.2 Secured Communication Mechanism

The designed security protocol utilizes the same link used for communication, with the main difference being that all messages exchanged are strongly encrypted and digitally signed by all participants. The vehicle and the station mutually authenticate each other prior to exchanging messages. Before initiating the communication process, the CA generates and approves all public and private keys for the vehicle as well as stations. The CA is considered an entity which is credible and trusted by all parties wishing to communicate. The CA generates the set of public and private keys for each and every vehicle separately and for the individual stations. The CA's public and private keys are used in the digital signature processes. Once the key generation is complete, every vehicle and each station are loaded with their corresponding public and private keys. The CA also distributes its public key to all vehicles and digitally signs the vehicle/station IDs, expiration date and their public keys using its public key. Expiration date is used for further verification of the vehicle and station, while an ID represents a unique number issued to the vehicle or station. Along with these keys, the vehicle collects and stores, using an onboard unit, all its sensor readings along with cargo details. With all the details ready, the truck initiates the communication process with a station. The nature of the message exchanged depends on the type of station communicated with (i.e. departing, weigh or arriving). The following outlines the main message sequence between the vehicle and the station during the inspection:

a) The vehicle receives the station's certificate and, using the preloaded CA's public key, verifies the station's certificate. If all the credentials (ID, expiration date, etc.) are found valid, the vehicle extracts the station's public key from the certificate. This assures the vehicle that it is communicating with the correct station and not an imposter. After obtaining the station's public key, the vehicle uses this public key to encrypt the unique 'Session Key' and send the same key to the station along with its certificate. The Session Key is the key used to encrypt the vehicle details, such as driver ID, cargo information, sensor readings and other related information using the DES algorithm. This key is unique and is generated each time the vehicle communicates with the station. Thus no two stations will receive the same session key. If, on the other hand, the station's details fail to be verified, the vehicle sends a message indicating "failure to validate key" and logs the result.
b) Upon receiving the vehicle's certificate, the station extracts the ID and expiration date of the vehicle using the CA's public key. If the received details are found valid, the station proceeds to the next set of messages. The station extracts the session key from the vehicle's certificate using its private key and decrypts the vehicle details using the session key. If any of these details fail to be correctly verified, the vehicle is not granted permission to proceed further and the result is logged.
c) Given properly credentialed and encrypted information, the station will make a determination of vehicle compliance, and then respond to the vehicle to indicate whether to proceed or stop.

This revised secured communication framework delivers all the required services mentioned above, including the verification of the parties' identity at each and every stage and at the same time maintains the confidentiality of the data through encryption. Vehicle details are 8 bytes in length while the cryptographic algorithms operate on data units of length 128 byte or above.

2. KEY TRANSPORT MECHANISM

As mentioned above, in the Trusted Truck® environment, there is an asymmetry between the computational capabilities of the truck and the stations. The truck is equipped with a low-grade, 16-bit processor while the stations are equipped with a PC-level processor system. This greatly varies the time taken by the truck to compute the cryptographic algorithms when compared to the station.

The major operations on the truck side as well as station's side are the signature generations, signature verifications and the encryption and decryption operations. The signature generation using RSA can be done by performing the following operation

$$S = M^{d} \bmod n \qquad (3.1)$$

where M denotes the message, d the private key, n the product of two large prime number p and q, and S is the signed message or encrypted message. The corresponding verification is accomplished by performing

$$M = S^{e} \bmod n \qquad (3.2)$$

where e is the public key or the decryption key. In the designed system, the decryption key is chosen to be $e = 3$. Lower value of e reduces the number of modular multiplications required and thus decreases the overall time taken to perform (3.2). The private and public keys of the vehicle and the station are 128-byte in length and those of the CA are 144-byte in length. The mathematical operations in (3.1) and (3.2) involve modular exponentiation [1], which is the core time-consuming function. In this system, all cryptographic algorithms operate on 128-byte numbers, so the vehicle with a simple 16-bit processor on board requires more time to compute the core operations when compared to the station which is equipped with a strong processor. Thus the other goal of the protocol would be to balance this asymmetry by intelligently optimizing the algorithms involved. Along with the speed-up in the algorithms, an innovative way of utilizing the travel time has been formulated, namely in the form of an offline key transport method, as described next.

4.1. Offline and Online Key Transport

In this method, the vehicle performs the operations in two modes-offline and online. Here offline refers to the stage where the vehicle is not in the vicinity of an inspection station or the time prior to reaching the next inspection station. The term online refers to the time interval during which the vehicle is communicating with the station and is located in its vicinity. The vehicle uses a method of offline key generation and an online key transportation to send the key to the station.

1.1.1 Offline Key Generation

In offline key Generation, the vehicle completes the generation of the session key and issues a certificate by signing a message (containing the session key and the vehicle ID) using the vehicle's public and private keys. As the session key is used for the encryption and decryption of critical messages, care has to be taken while transporting the session key to the station. Instead of sending the message directly, a message V is framed with the session key in it such that only that specific station is able to recover V and at the same time the station must be assured that a particular and unique vehicle generated message V. If K (8 bytes) is the session key, then the message V (128 bytes) is framed such that

V = {64 bytes of zeros || 4 repetitions of VehicleID ||
4 repetitions of K}
(3.3)

This message is digitally signed using the (n_t, d_t) pair,

$$L = V^{d_t} mod\ n_t \qquad (3.4)$$

where (n_t, d_t) is the public and private key pair of the vehicle and L is the digital signature of the message V. The repetitions of the ID and the session key in the original message prevent intruders from modifying the message. The number of repetitions of the ID signifies the known message which is embedded in the original message. The other reason for this message framing is that, the station after using the modular exponentiation for verification (equation (3.6)), is left out with the last 64bytes of data which contains the vehicle ID and the session key. Moreover, unlike the standard RSA [6] protocol; here we cannot transmit the original message for signature verification as it contains the secret key (session key). So even the signature is encrypted using the station's public key and later this key is recovered from the extracted message. Let C be the encrypted version of the signed message, then C is given by,

$$C = L^{3}\ mod\ n_s \qquad (3.5)$$

where n_s is the station's public key. When the vehicle approaches an inspection station, after authenticating the station, the vehicle sends the session key and it's ID via the online key transport mechanism.

1.1.2 Online Key Transport

In Online key transport mechanism, the station verifies the vehicle and the latter signs the offline generated certificate (containing the session key) using the station's public key. Next, it sends this signed certificate to the station. The certificate is transmitted to the station and upon verification, the station verifies the data sent from the vehicle and issues a decision. As generation of this certificate takes less time when compared to the offline certificate and also requires the station's verification, the vehicle performs this process online.

1.1.3 Session-Key Recovery

In Session Key Recovery the station recovers the session key and decrypts the messages sent by the vehicle by decrypting the signed certificate using the station's public key,

$$V = \{C^{d_s}\ mod\ n_s\}^{3}\ mod\ n_t \quad n_t < n_s \qquad (3.6)$$

The station extracts the session key from the message V. This innovative way of generating the key offline and performing the computations before approaching the station reduces the load on the vehicle as well as saves time for the inspection station.

2. COMPUTATIONAL CHALLENGES AND PROPOSED SOLUTION

In order to overcome the inherent resource imbalance between the vehicles and stations, techniques were used which exploited the asymmetry characteristics. One of the key solutions is the incorporation of the offline key transport method, wherein all the time consuming operations were computed ahead of the communication session. The other important solution is the application of the Chinese Remainder Theorem on the vehicle's side. The modular exponentiation has a higher order of complexity and also consumes more time compared to other calculations. The Chinese Remainder Theorem (CRT) optimizes the time required to perform modular exponentiation, thus speeding up the RSA process. The CRT technique breaks down the exponentiation into parts and then combines them.

By utilizing the CRT, we reduce the time taken for the modular exponentiation by a factor of 4 times. An efficient algorithm for the CRT is described in [6]. We have observed the following:

- *The time taken for modular exponentiation on a 32-bit processor without CRT is approximately 0.25 seconds*
- *The time taken for modular exponentiation on the 16-bit processor without CRT is approximately 0.45 seconds*

This time difference causes a great asymmetry in the communication process whereby the station should be validating a number of vehicles concurrently. In order to balance this inequality, optimizations are made in several ways on the vehicle side. This is done in an attempt to reduce the computational load on the truck, which introduces several constraints at the CA level on the keys generated for the truck. When the CA generates the public and private keys for the truck, it ensures that those keys are always less than the keys generated for the station so that the values calculated on the truck are always less than that at the stations and always take less time.

Let p_t and q_t denote the prime numbers generated for the vehicle and p_s and q_s be the prime numbers for the station. To ensure that the above relational inequality is maintained, the second most significant bits of p_t and q_t are always made zero and that of p_s and q_s are always made 1 (one). As a result, the prime numbers for the vehicle take on the form $(10p_2p_3p_4......1)_2$ and the prime numbers for the station take on the form $(11p_2p_3p_4......1)_2$. As the numbers are prime in nature, the LSB and MSB will always be 1. All trucks perform the session key generation required for the authentication phase offline. This offline key generation is performed for every communication session before approaching a station, thus saving crucial time. On the other hand, the stations perform all the operations online. The only operation performed by the truck online is the modular exponentiation with the exponent equal to 3, i.e. $A = B^3 \text{ mod } N$ where A, B and N are 128 byte numbers. Mathematically, as the operation $A = B^3 \text{ mod } N$ simply involves one modulo calculation, it takes far very less time when compared to the operation $A = B^E \text{ mod } N$. Thus, when the truck initiates communicating with the station, it does not have to spend much time on computations. The combination of these techniques reduce the computational load on the vehicle and help the vehicle in completing the processing required in a reasonable time frame in the order of hundreds of milliseconds. Upon implementing the CRT on the vehicle, the time taken for the modular exponentiations is greatly reduced.

1. RESULTS

The proposed data security protocol was implemented in ANSI C with no requirement of any additional software components. The computational time is noted at each and every stage in process involved and proper care is taken in selecting the appropriate cryptographic algorithms which will fit the environment. The time taken for the modular exponentiations in both 32 bit and 16 bit is observed and noted. Table 1 details the processing times observed on the stations (32-bit processor) platform in performing modular exponentiation, when implemented both with and without the CRT.

Table 1. Time Estimate for modular exponentiation on a 32-bit processor with and without using CRT

Trial No.	Processing time w/o CRT (secs.)	Processing time with CRT (secs.)
1	0.208438	0.057042
2	0.223449	0.057879
3	0.206945	0.057248
4	0.215324	0.056165
5	0.229685	0.056701
6	0.226190	0.056904
7	0.233663	0.058223
8	0.224079	0.05743
9	0.212913	0.056463
10	0.205311	0.057443
Average	**0.2186**	**0.05715**

However, in this application, the participant that requires speed up is the vehicle which utilizes a simple 16-bit processor. It is found that the average processing time required by the 16-bit processor to compute the equation $S = M^d \text{ mod } n$ without using CRT is in the range of 400 to 500 milliseconds. When CRT is employed, the same computation task is achieved in 120 to 130 milliseconds.

2. CONCLUSIONS

In this paper, a successfully deployed novel data security protocol for the Trusted Truck® system is described. The innovative claims involve an offline key transport method which significantly reduces the computational load imposed on the vehicles in real-time. The security services offered include data integrity as well as authentication. The protocol is designed in a way that facilitates embedding of the code in the existing architecture of the Trusted Truck® system without need for any additional hardware or software.

3. ACKNOWLEDGEMENT

This work has been supported by research grant DTRT-06-G-0043-03-U22-06-01 from the National Transportation Research Center (NTRCI), Inc.

4. REFERENCES

[1] Bruce Schneider "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Second Edition 1996.

[2] Introduction to cryptography with coding theory, second edition Wade Trappe, Lawrence C. Washington 2006.

[3] Data Encryption Standard, Federal Information Processing- T. Takagi, "Fast RSA-Type Cryptosystem Modulo pkq", CryptoStandards Publication (FIPS PUB) 46, National Bureau of Standards, 1998, 1462 of LNCS. 1998, pp. 318-326.Washington, DC (1977).

[4] M.O. Rabin .Digital Signatures," Foundations of Secure Communication, New York: Academic Press, 1978, pp.155-168.

[5] R.L. Rivest, A. Shamir, and L.M. Adleman, "On Digital Signatures and Public Key Cryptosystems," MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212, Jan 1979.

[6] Handbook of Applied Cryptography Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone 1996.

[7] Trusted Truck® Environment, http://www.ntrci.org/