a printout may be obtained showing these and other data. The owner/operator may obtain an indication of the period of time the vehicle is operated in excess of the 65 mile per hour overspeed limit. Similarly, apparatus disclosed by Ishibashi, US Patent No. 5,379,219, and Komatsu, US Patent No. 5,249,127 suggest the tracking of speed over time and, per Figure 3 of the '219 patent, the allocation of memory among ID data, speed data, travel distance data and optional area. The '127 patent suggests that, memory size requirements being indeterminate and expensive, data compression devices be provided for assuring efficient utilization of memory.

It has further been recognized that portability of the collected data is required. One means of achieving portability is via an external memory module (US 4,757,454, 5,185,700 or 5,249,127). Also, radio or generally wireless radio communication may provide data mobility from one user to another (US 4,804,937, 5,185,700 or WO 90/09645).

The so-called global positioning system described, for example, by Taylor et al., US Patent No. 4,445,118 and O'Neil et al. US Patent No. 4,839,656 has been implemented in an electronic vehicle log by Haendel et al., US Patent No. 5,359,528. Haendel et al. describe that a change in state boundary and a log of miles within a particular state may be automatically obtained without driver intervention.

All of these systems suffer from a lack of security of access by a particular user and may be falsified if and when the provided weak security systems fail. It is an object therefore of the present invention to describe a system whereby multiple users of a system may configure or obtain access to memory of an electronic vehicle log. It is a further object of the present invention to provide a system wherein security is enhanced via adaptation of evolving technologies of speech recognition and speaker verification, public/private key data encryption and decryption, flash or smart card (key) access and/or electronic signature record verification and access.

SUMMARY OF THE PRESENT INVENTION

In accordance with the present invention, an electronic vehicle log (EVL) comprises a processor for processing data, a memory for storing software algorithms and fixed data, preferably non-volatile in nature, a secret key unique to the vehicle log, and a unit serial number that is unique to that unit (hereinafter, an EVL identifier), a removable non-volatile log memory for securely recording data and a

navigation and time-of-day and date input data circuit. In one embodiment, there may be further provided a microphone input for receiving user speech coupled to the processor (for example, via an analog to digital converter) and a memory for storing digitized voice samples. Optional sensors are coupled to the log for providing for the input of data for vehicle and cargo, for example, through an external interface, in particular, a wireless interface. For example, through one external wireless interface, an EVL may acquire event data such as weight-in-motion (WIM) data. Those who would obtain access to data or input data are provided with a public key which is likewise unique to the vehicle log. Moreover, any data entries are signed with an electronic signature for verifying the entered data, for example, comprising a calculated hash value encrypted with the secret key.

When the vehicle is to be used, the driver inserts the removable non-volatile log memory for the duration of the trip. For example, a driver may obtain access and log into the EVL by inputing their speech, a password or a biometric after inserting their card memory. Upon successful verification of the password or biometric and, if appropriate, verification of the speaker's identity in a well known manner, the driver-unique data is used to decrypt a secret key member of a public key encryption pair. When data is to be logged by the driver, protected data packets (PDP's) containing this log data are generated with digital signatures formed by encrypting digital hash values with this secret key member of the public key pair.

Protected data packets (PDP's) are transmitted to a requesting user via electronic means, for example, wireless, telephone modem or a memory card. The requesting user has a trusted (escrowed) copy of the public key of the above-referenced public key pair, the public key pair including the secret key (securely stored in and never released from EVL memory) used for forming the electronic signature. The secret key should be protected and secured as closely as possible and should not be transmitted (otherwise, it might be intercepted by an uncertified individual). The public key is used to verify that the electronic signature of the PDP is accurate. Correct verification of the electronic signature then confirms the data source (the driver-protected secret key) and the integrity of the data (since the hash value matches the PDP data).

A governmental authority may obtain access by a defined process. One

example of such a process for obtaining an early transmission of vehicle data in advance of a border crossing or like event is described by the following. The agency wishing to receive secure data generates a public key encryption pair different from that used by the driver and distributes the public key portion to any person or system desiring to transmit secure data. The public key portion is stored in EVL memory. A profile of a commercial vehicle and a cargo may be extracted from the vehicle via a card memory or may be electronically extracted by wireless means prior to the vehicle's departure and delivered to the authority with the stored public key portion. The EVL generates a private encryption key and uses it to encrypt PDP's with their corresponding digital signatures. The EVL encrypts this private encryption key using the public key and transmits that information to the agency receiving the data. The receiving agency decrypts the EVL private encryption key using the secret key portion of the key pair and then decrypts the PDP's using the decrypted key. The profile and public key are transmitted via a centralized authority data base to regional data bases for distribution to checkpoints, port of entry border crossings and the like along the intended route of the vehicle.

As the vehicle approaches the inspection facility, the vehicle is polled or interrogated, for example, preferably by wireless means in advance of reaching the facility, so the vehicle need not stop its movement. The vehicle transmitted profile data is compared with the previously transmitted profile data and the inspector may preclear the vehicle through the inspection station. If the inspection data is a weigh station, for example, and data is to be entered into the log by the authority, an electronic signature is utilized to verify the entered data, preventing subsequent modifications of the logged information. Moreover, at the time the entry is made, the vehicle position and time from the global positioning system may be automatically and simultaneously recorded, allowing detection of fraudulent entries. As the vehicle crosses the border, a short range communications system may be used to verify that the vehicle crossing the border is the vehicle which received the preclearnace to cross.

It is also possible that the vehicle may carry all the profile information in the EVL and transmit the data via wireless means to the authority just a few minutes before the approval (for example, preapproval at a border crossing) event. In this

case and in that described above as well, some sort of short-range transmission is useful as the vehicle crosses the border to physically confirm that the vehicle currently crossing the border is the same as the one that provided the profile and credentials and received preapproval to cross.

An authorized individual such as an inspector or police officer creates a digital credential in a generating device's memory, for example, a laptop personal computer. A secret key of a public key pair is used to generate a digital signature for the credential data. The credential and signature are transmitted to the EVL using various means, possibly including wireless means, direct input (typing), or memory card transfer. This transfer may be encrypted as discussed above as desired. for wireless or other secure data transmission. The credential and signature are formed into a PDP and logged as described above for the driver data logging operation. When the credential is subsequently transmitted to a requesting agency, the agency will use a trusted copy of the public key portion to verify the electronic signature of the PDP.

Other features and advantages of the present invention will be explained by reference to the drawings and the following detailed description of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an overview drawing of an electronic vehicle log according to the present invention;

Figure 2A is a system overview drawing showing the interface between a vehicle 200 carrying an electronic vehicle log of Figure 1 with a governmental or other authority and Figure 2B shows vehicle 200 with expanded boxes describing data that may be stored in DPIU 210 including an electronic vehicle log of the present invention;

Figure 3 is a schematic block diagram of the electronic vehicle log of Figure 1 for maintenance in a vehicle; Figure 3A provides a first embodiment, Figure 3B provides a second embodiment and Figure 3C provides a third embodiment;

Figure 4A provides an overview of the key and security features of the present invention in flow diagram form and Figure 4B shows a table showing the use of different public key pairs by different entities for accessing the data stored in the EVL

400 of Figure 4A;

Figure 5A provides a table of examples of data maintained in an in-vehicle data base of memory of the in-vehicle unit of Figure 4; Figure 5B comprises a table showing data elements and characteristics recoverable through utilization of the present invention and their characteristics; and

Figures 6A and 6B provide a table showing service, application, technology or product availability, demonstrable feature and utilization of the present invention.

DETAILED DESCRIPTION OF THE PRESENT INVENTION

Referring to Figure 1, there is shown an overview drawing of the electronic vehicle log of the present invention. The present device is intended to be placed in a vehicle, hence, the present invention is described herein as an in-vehicle data processing unit. The log is described herein as electronic because it generally operates via electronic circuits including at least memory circuits and a data processor. The present invention is characterized as a log because the memory of the present invention substitutes for prior art hand-written log books typically used by drivers of vehicles, especially commercial vehicles.

The electronic vehicle log (EVL) 1 is described by box 1a as comprising a package of elements suitably housed to be mounted in a vehicle, for example, in an operator compartment or secure area therein or proximate thereto. One mounting arrangement would be to provide a bracket mounting plate permanently secured to the vehicle. The EVL housing, herein referred to as a data processing interface unit (DPIU) then is removably secured thereto by mechanical locking apparatus so that the DPIU may be removed from the vehicle as necessary. The mechanical locking apparatus should be tamper-resistant so that the EVL itself cannot be surreptitiously moved from one vehicle to another without detection. (To accomplish this objective, electronic tamper detection may be employed). Preferably, the DPIU housing is adapted to receive a removable security module as will be further described herein which is the electronic vehicle log itself.

The EVL housing 1 (DPIU) contains a processor, preferably a microprocessor and a non-volatile memory coupled thereto for storing at least secret key data, secret EVL unit serial number data and executable software. The EVL 1 further may comprise a random access memory that typically is volatile for storing data on a

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.