NEUTRAL VEHICLE PLATFORM

Technical Concept

Neutral Vehicle Working Group

Content

Introduction

The vehicle ownership experience is dynamically changing with new models of transportation and mobility as a service evolving rapidly. Electrification, shared economy, autonomous driving and an exploding range of "smart" tools and services - enabled by vehicle generated data - are challenging organizations to have a well thought out data strategy. Today, access to data already is the key to innovation and creating competitive advantage; in the future, it will be a matter of survival. That is why "access to data" has become *the* topic in the transportation industry.

In this context, a major concern has there been raised over some vehicle manufacturers limiting/controlling access to vehicle data and thereby making it more difficult, if not impossible, for vehicle owners, fleet managers and third party product and service providers to compete, innovate, or even participate in the marketplace. One prominent example is a server based system known as "Extended Vehicle" which has created fears that it would concentrate data access with one stakeholder. As a result, a diverse array of stakeholders in the mobility ecosystem have asked for a data access model that would preserve the existing "neutral", direct access to real time vehicle data and provide the freedom for all stakeholders to create value while advancing cybersecurity. In response to this, the Neutral Vehicle Working Group has put forward a "neutral" data access model that, in addition to neutral data for free competition purposes, would also enable the use of data analytics in the public interest, including carbon footprint reduction, traffic and accident management, and services for smart communities.

The industry and public policy aspects of this issue are outlined in more detail in the White Paper "Keeping the Connected Car Connected Q&A - Innovation, Competition and Security in Data-Enabled, Digital Mobility."

In this paper, we are pleased to present the next iteration of Neutral Vehicle Technical Concept which is being developed in parallel. Its initial reception has encouraged us to keep advancing the work. As a highly collaborative, multi-stakeholder initiative we are grateful for feedback and looking forward to more input as we are seek to integrate provider neutral (and competing) approaches in support of the overall mission of neutral, secure and direct access to rich, high quality data. On the data handling side, that goal requires broad industry standards for security, privacy and data quality and we have placed a lot focus here. In addition, mobility data needs a common language. In order to leverage third-party applications, platform standards need to be open (Open API), inexpensive and broadly available. This can be achieved through an open port in the vehicle or a shared web service.

Our thanks for providing initial critical review and guidance go to Mr. Neil Cawse, founder and CEO of Geotab Inc.; Dan Massey, Professor at University of Colorado Boulder and former program manager in the U.S. Dept. of Homeland Security Science and Technology Directorate Cyber Security Division (including cyber security for automobiles); Derik Reiser, Assistant Vice President, IT Architecture & Innovation, Enterprise Holdings Inc.; Ted Guild, Automotive Lead at World Wide Web Consortium (W3C) and Research Staff at MIT Computer Science and Artificial Intelligence Laboratory (CSAIL); and Mr. Craig Smith, Research Director of Transportation Security at Rapid7 and author of *The Car Hacker's Handbook*.

Please keep the feedback coming - we value your ideas, questions and criticism. This is what will make the Neutral Vehicle robust and sustainable.

Stefano Peduzzi
Neutral Vehicle Working Group

Guiding Principles

The Neutral Vehicle Platform proposal has been developed according to the five guiding principles identified by the EU Commission C-ITS platform project.[1]

Generally, vehicle ownership should convey the right to access vehicle-generated data directly, in real-time and independently from the OEM. Access to data enables the vehicle's owner to participate or leverage products, services and functionality, including (but not limited to) maintenance, repair and online services (such as navigation, telematics, e-call after accidents, autonomous driving, entertainment, smart door lock/unlock, remote starting, etc). The EU Commission report produced a series of recommendations that have been included for the Neutral Data Platform:

- Platform "neutrality" must be sustained well into the future — while Geotab feels uniquely qualified to play a leading role in platform development, setup, and maintenance, the platform must not depend on a single provider.
- "Neutral" implies a high degree of interoperability. Platform design must be open and modular so that different providers can connect and operate their products and/or platform components — this is a platform for competitiveness.
- Platform governance should be placed under the oversight of users/stakeholders.
- Focus of oversight will be security, privacy, and interoperability.
- Interoperability must be a key design feature of the platform.
- Platform must be interoperable with hardware and software of reputable providers (i.e. those who meet industry sanctioned security standards).
- Compliance with European standards, in particular on data privacy, is critical. Enable compliance with EU data laws and in particular GDPR and facilitate a variety of data use cases with differing levels of privacy impact based on context and user preferences.

[1] C-ITS Platform Final Report (2016)

Technical Architecture

The Neutral Vehicle Platform provides an end-to-end framework for transferring rich vehicle data from the ground to the cloud and back, allowing development of advanced applications and services by 3rd parties. It is based on the concepts of openness, security and interoperability:

Openness:

- The Neutral Vehicle Platform allows interoperability with different telematics hardware, software providers (operating systems and hypervisors), and OEM solutions.
- It allows different service providers to continuously innovate and develop applications to end users using a common set of APIs and a common Vehicle Data Set.

Security:

- The security requirements for access to in-vehicle data and resources and the security requirements for applications and service are based on advanced industry best practices, recommendations and standards, and are regularly reviewed, tested and updated as part of the security governance framework.
- All the information collected and all the communications are encrypted using state of the art guidelines, protocols and standards.
- Availability of data to application and service providers is subject to vehicle owner formal approval and compliance with privacy regulations.

Interoperability:

- The platform documentation and SDK are publicly available.
- The platform provides a set of APIs based on common standards as REST and JSON that facilitates an efficient data exchange.
- The platform defines a Common Vehicle Data Set that abstracts both the "physical layer" (vehicle make/model) and technology used to access the in-vehicle data and resources.
- The platform runs on a cloud environment and can easily scale horizontally.

Overall the technical architecture of the platform can be summarized through the following four components:

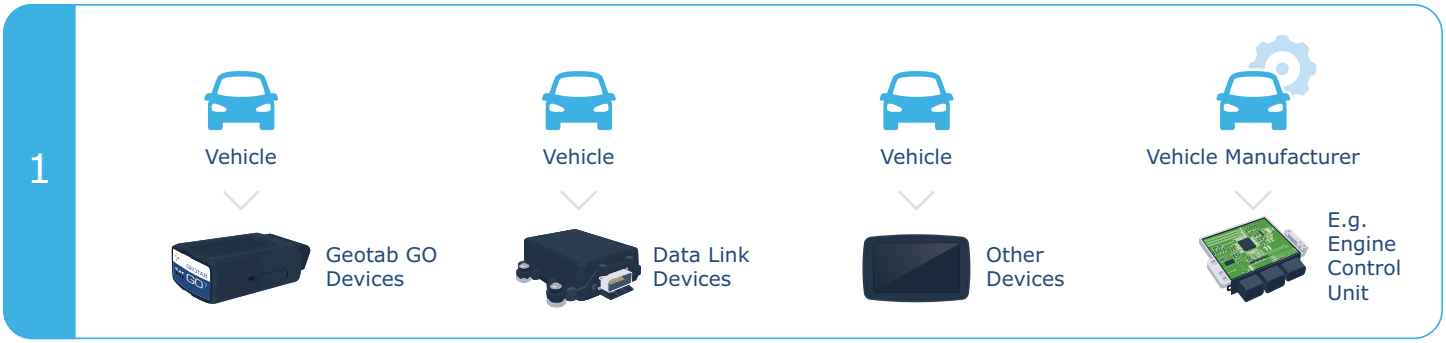
1. In-Vehicle Data and Resources Access Component
2. Vehicle to Cloud Component
3. Neutral Server
4. Application and Services Component

NEUTRAL VEHICLE PLATFORM

Components Description

There are multiple roles being represented in the outlined concept. However, one organization could be generating data, be certified to provide a Neutral Vehicle Platform service and build products upon the data to market those.

In-Vehicle Data and Resources Access Component



Real-time data collection and access to the vehicle resources can be either conducted via an aftermarket telematics device or through embedded in-vehicle technology. In particular the following options are identified:

- OBD and Secure Vehicle Interface based devices
- CAN Contact-less based devices
- On-Board Applications (OTP, HyperVisor)
- Manufacturer Specific devices or on-board applications

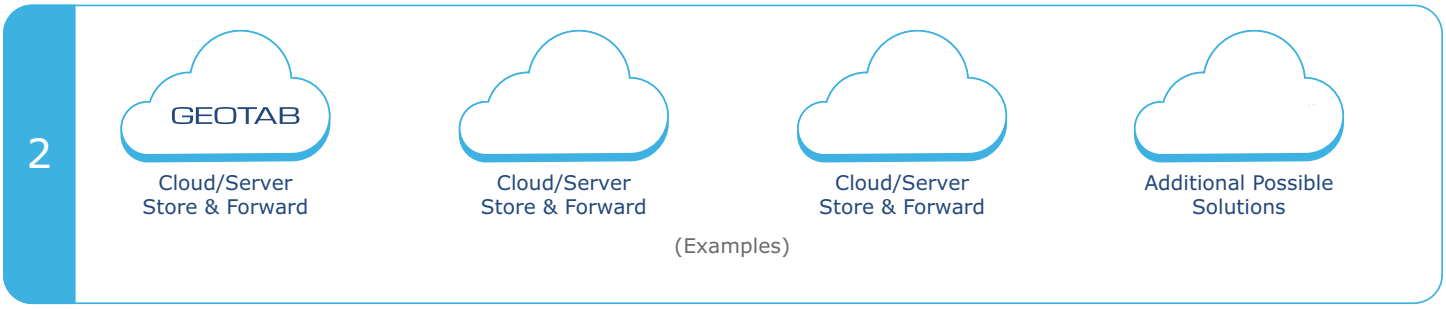
All the solutions have to adhere and follow a regulated set of security principles and follow secure design practices:

- Third-party Auditing: All security-relevant components of the system should be audited appropriately and audit results should be provided to the Neutral Vehicle Platform governing body.
- Kerckhoffs Principle: Security elements should be designed assuming the attacker has full knowledge of the device or application and already has full access to the code.
- Availability: Device firmware and applications should be updatable and maintained by the solution provider.
- Authenticity: All device firmware and application updates must be digitally signed: signing application updates verify that the updates have come from a trusted source. Acceptable algorithms to use for the signature are based on NIST recommendations.[2]
- Random Number Generation: Device firmware and applications should use cryptographically strong random numbers.
- Distinct Keys: Different keys should be used for different roles. For example, the same key should not be used for socket communication as for the application signature.
- Secure Data Transfer: Socket data encryption provides data encryption regardless of the state of the cellular network or any other intermediate connection medium.
- Implementing mutual authentication will verify that the received/transmitted data sources and destinations are legitimate. Acceptable encryption and authentication algorithms are based on NIST recommendations.[3]

Certification of authorized In-Vehicle Data and Resources Access Component is managed by the Governance body of the Neutral Vehicle Platform.

[2,3] E. Barker, "National Institute of Standards and Technology Special Publication 800-57 Part 1, Revision 4. Recommendation for Key Management," Jan. 2016

Vehicle to Cloud Component



The Vehicle to Cloud component acts as a bridge between the In-Vehicle Data and Resources Access Component and the Neutral Vehicle Server. This may also include a peer-to-peer secure cloud server connection or hybrid of both (ie. vehicle to cloud or cloud server to cloud server) to incorporate all use cases. The key functionalities provided by the component are:

- Manages the devices and applications provisioning and configuration.
- Manages the direct and encrypted socket connection with the In-Vehicle Access Component: different solutions can implement different strategies for connection (always on, time based, event based).
- Manages the security keys for the device or application.
- Manages the Over The Air (OTA) firmware and application updates for the In-Vehicle Access Component: responsibility for the updates lies with the solution provider.
- Monitor the health status of the In-Vehicle Access Component: the component is capable to identify faulty device, anomalies in the behaviour of device firmware and applications.
- Allows the development of application and services outside of the Neutral Vehicle Platform.
- Translates solution provider specific data set to the Neutral Vehicle Platform Common Vehicle Data Set.
- Filters the data set received from the In-Vehicle Access Component to only include the information for which the data subject provided authorization and consent to be used by the Neutral Vehicle Platform.

Manages the data transfer with the Neutral Server using the API provided by the platform.

In addition, the Vehicle to Cloud component must adhere and follow the regulated set of security principles and follow the secure design practices defined for the In-Vehicle Access Component. Additional principles and practices are defined for this component as:

- Internal account hierarchy should be implemented to limit server access, allowing access to back-end servers/ features to only those individuals who need them.
- Multi-factor authentication should be used for access control.

Neutral Server Component

Neutral data exchange is a key feature of the Neutral Vehicle platform. One architectural option to achieve this is the Neutral Server which facilitates interaction between vehicle data access components and applications and services providers. The Neutral Server includes a web server to serve the API requests, an application server to process the incoming data, and a database server to host the different data sets.

The key functionalities provided by this component are:

- Manages the provisioning of new vehicles (In-vehicle Access Component), new Vehicle to Cloud Components and new Application and services Components.
- Authenticates Vehicle to Cloud Components and Application and Services Components.
- Holds the authorization details for each Vehicle to Cloud Component and each Application or Service Component
- Processes the incoming/outgoing data from/to the Vehicle to Cloud Components:
  - Incoming data is routed to the different repositories for which the data subject has provided consent (specific Applications or Services and Big Data).
  - Incoming data routed to the Big Data repository is further processed and anonymized to ensure privacy of the data subject is respected.
  - Outgoing data is placed in the outgoing queue of the Vehicle to Cloud component associated with a particular vehicle.
- Creates, manages and stores a single separate distinct and isolated encrypted databases for each Application and Service Provider Component.
- Exposes a set of API that can be used by Vehicle to Cloud Components.
- Exposes a set of API that can be used by Application and Service Provider suppliers to access specific In-vehicle Access Component data.
- Exposes a set of API that can be used by Application and Service Provider suppliers to access Big Data datasets.

API

API requests made to the Neutral Vehicle Server are performed over HTTPS. API request parameters and the results are transported in the lightweight JSON format. The API reference contains a listing of the methods that can be invoked, the parameters they expect and the results they return.

Requests to the API can be invoked using HTTP GET or POST. HTTP POST requests uses the JSON-RPC standard.

The Neutral Vehicle Server API only allows making requests over secure connections (HTTPS). The minimum SSL/TLS version supported by the Neutral Vehicle Server API is TLS v1.2.

Common Vehicle Data Set

The Common Vehicle Data Set allows developers to completely abstract the specific vehicle make and model and the specific In-Vehicle Data and Resources Access Component used in the vehicle, highly facilitating creation of cross brand and hardware agnostic applications and services.

- While several data classification initiatives are discussed today by organizations like ETSI[4] or ISO[5] , the platform adopts a flexible model that allows to cater for the following type of information:
- Vehicle internal status data: this data can be generated by either vehicle sensors or by the sensors provided by the In-Vehicle Component and is related to the current condition of the vehicle. Examples: Odometer, Speed, RPM, Longitudinal Acceleration, Lateral Acceleration, Fuel Level, Distance to Maintenance, Active DTC/Fault Codes, Lights, Location, …). Typically this data is fast changing and will change several times during a trip

---

[4] ETSI TS 102 894-2 - Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary

[5] ISO/TS 19321:2015 Preview Intelligent transport systems -- Cooperative ITS -- Dictionary of in-vehicle information (IVI) data structures

- Vehicle external status data: this data can be generated but either vehicle sensors or by the sensors provide by the In-Vehicle Component and is related to the current conditions outside of the vehicle. Examples: Ambient temperature, Rain sensor, Traffic Light, Traffic Signs, Road lanes). Typically this data is fast changing and will change several times during a trip
- Vehicle identification data: this data allows to identify the vehicle and its components. Examples: VIN, ECUs (Name, Serial Number, SW version), Registration Number. This data is usually slow changing or not changing during the life of the vehicle.
- User introduced data: this data allows to identify vehicle data that is specific for the current driver. Examples: SatNav destination, Radio station, A/C settings, Seat position. Typically this data is fast changing and will change one or more times during a trip

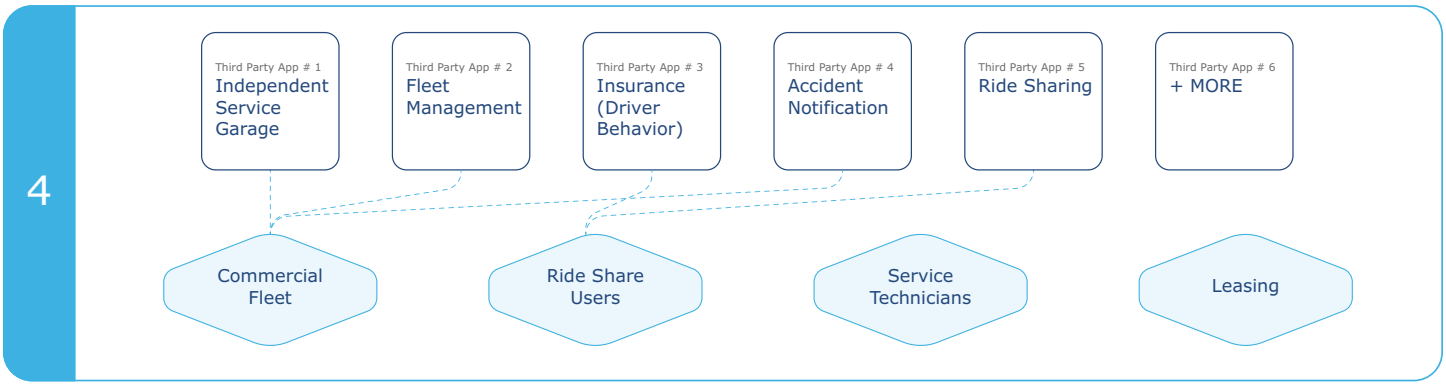
Fast changing data is managed via the Status Data, Fault Data and Log Record objects.

Slow changing data is managed via the Device and Custom Data objects.

Each object is defined by a set of properties specified in the platform SDK.

For each Status Data the Common Vehicle Data Set provides a Diagnostic object that includes the descriptive name, identifier, definition, unit of measurement and details on the source of the data.

Application and Services Component



Each Application and Service developed by third parties is certified by the Governance body and must comply with a set of specified standards for security and privacy.

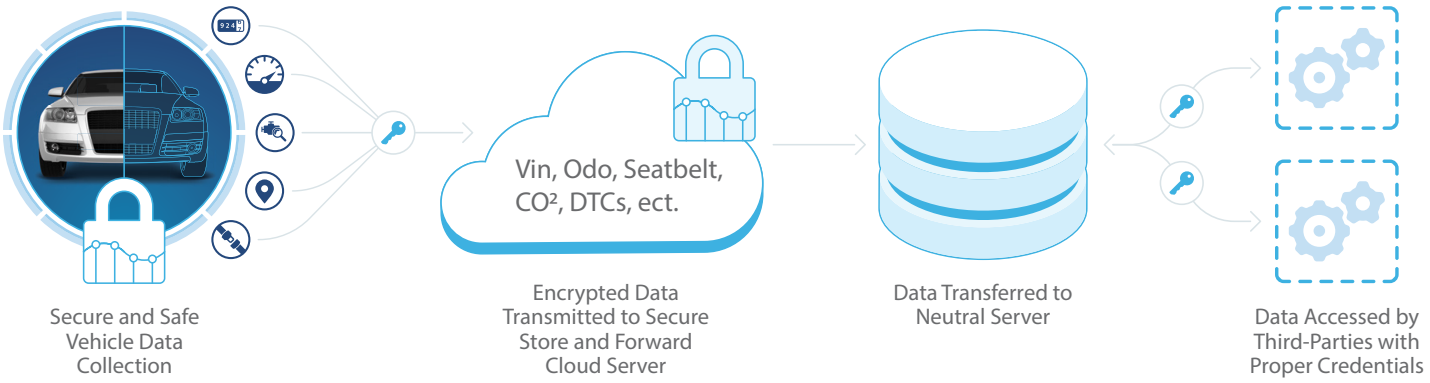
Once certification is achieved, the third parties will be able to publish their application or service on the Neutral Vehicle Platform marketplace.

Application and Services interact with the Neutral Server in two ways:

- Authentication
- API calls for
  - Provisioning of new vehicles for a specific Application or Service
  - Data retrieval from vehicles
  - Requests to utilize vehicle Resources
  - Big Data dataset retrieval

In case of Applications and Services that utilize vehicle specific data, they have to include the functionality for the data subject to grant authorization to specific Common Vehicle Data of the vehicle. The authorization is used to provision a new vehicle and defines the rules for delivery of vehicle specific data in the Application or Service database.

Security Characteristics



There can be no doubt that security is the most important aspect to the Neutral Vehicle Platform. A comprehensive, standards based end-to-end cyber security program is required. The cyber security program implemented by the platform includes Secure and Safe Vehicle Data Collection, Encrypted Data Transmission, Secure Data Transfer to a Neutral Server, and the appropriate Authentication, Authorization, and Security Controls for secure data access.

The Neutral Vehicle Platform cybersecurity program allows to continuously adapt and continue to implement cutting edge technology as technology and cyber threats evolve.

In order to ensure the end user data confidentiality, integrity, and availability the following principles are required:

- Self serve data: Vendors system and data access should be for support and maintenance only. Users must have the ability to retrieve their own data without Vendor assistance.
- Data resilience: End users control the amount of personal data collected by the system. The platform must be designed to function with end users who provide minimal or no personal data.
- End user data sovereignty: The end user claims all data ownership rights. This explicitly excludes data ownership rights for any organization or entity other than the end user.

Reducing residual risk to an acceptable level is one of the key goals of a security program. The following fifteen recommendations (15 Security Recommendations for Building a Telematics Platform Resilient to Cyber Threats) should be implemented on the Secure and Safe Vehicle Data Collection level. Following the recommendations is a proactive step towards reducing residual risk in data collection.

Governance

As the Neutral Vehicle Platform is intended to meet the digital needs of the broader mobility ecosystem well into the future, a robust system of governance must be part of the initial design. In a way, the Neutral Vehicle could well become the epicenter of connecting vehicle data generation with digital mobility product providers and users, many of whom can be both in competition and cooperation with each other. In addition, the Neutral Vehicle must have credibility with key stakeholders such as vehicle manufacturers, cyber security and safety agencies, and data protection authorities.

The governance of the Neutral Vehicle should therefore encompass oversight in the following areas:

1. Cyber Security — Ensure ongoing development and implementation of advanced cyber security standards and practices.
2. Data Privacy — Ensure that the Neutral Vehicle Platform meets all applicable privacy requirements under the coming GDPR.
3. Competitive Data Access for Broad User and Provider Ecosystem — Ensure neutrality by enabling an innovative and competitive marketplace for data driven mobility.

4. Long-term Neutrality — Allow relevance of the Neutral Vehicle in a changing technological, regulatory and market environment.

Cyber governance could include both oversight provided under the auspices of a credible associations and/or include an oversight board consisting of respected cyber security/cyber security management experts from industry, standards organizations, industry associations, academia and government.

General and privacy governance could be provided by a neutral body or association currently in existence or include a dedicated oversight board with representatives from key members of the ecosystem.

While it is anticipated the Neutral Vehicle Platform will be developed and operated by a commercial telematics provider with large scale platform expertise (or a consortium of providers), the governance design must include the appropriate licensing regime to ensure platform neutrality and independence into the future. The commercial arrangement must ensure that costs of platform development and operation are appropriately covered - in particular to allow for a high quality/high functionality system with ongoing innovation — and at the same time ensure competitive (including cost competitive) access for ecosystem participants.

Geotab's Role in the Neutral Vehicle Project

Geotab is a global expert in large scale, advanced telematics platform and related ecosystem design and management as well as a proactive collaborator in cross-stakeholder/industry security program advancement. Geotab is pleased to act as a catalyst and facilitator for the initial concept, design, and development of a stakeholder driven Neutral Vehicle Project and consider additional roles further down the road.

For more information, please contact: info@neutralvehicle.com