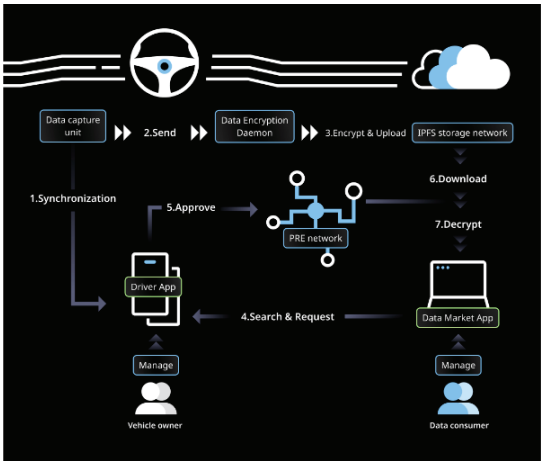
Privacy-preserving automotive data sharing to accelerate mobility service innovation

Public report



Project within FFI Transport and Mobility Services

Authors: Lei Chen (RISE), David Jiao (Privasea AB), Mathias Johanson (Alkit Communications AB)

Date: 2023-07-31

FFI Fordonsstrategisk Forskning och Innovation

VINNOVA Energimyndigheten TRAFIKVERKET FKG VOLVO SCANIA VOLVO

Content

1. Summary

Mobility is under transformation with increased automation, connectivity, and intelligence. One of the key assets that enable future sustainable mobility solutions is the data generated by the vehicles. Despite the consensus on the importance of vehicle data and the positive attitude toward vehicle data sharing, key challenges have always been on how to motivate data sharing, how to protect the data security, privacy, and integrity, how to comply with the EU and local regulations, and what the business models look like. The need for methods and platforms to address such challenges is urgent to support the design of new mobility solutions for sustainable transport and new business potentials to maximize the data value.

The project focuses on automotive data sharing and conducts firstly an analysis of data sharing within the vehicle and transport sector, followed by an investigation of the forthcoming Data Act introduced by the European Commission on how it might affect the existing data ecosystem of the automotive industry. The emerging blockchain technology and the rapidly developed tokenized economy are investigated for their potential to support data sharing and a data-driven economy. Following the analysis, the project focuses on integrating advanced encryption technologies, blockchain technologies, and Web 3.0 for a data-sharing platform to support secure and privacy-preserving automotive data sharing. Privacy-preserving data sharing (PPDS) is thus proposed with different architectures integrating various emerging technologies for exploring automotive data values.

A prototype is developed based on advanced encryption and blockchain technologies and demonstrated. The proposed PPDS allows highly secure and privacy-preserving data sharing that complies with GDPR and encourages data owners to share data through the tokenized economy, thus accelerating data-driven innovation in the mobility and transport sector.

2. Sammanfattning på svenska

Mobilitet är under transformation med ökad automatisering, uppkoppling och intelligens. En av de viktigaste tillgångarna som möjliggör framtida hållbara mobilitetslösningar är den data som genereras av fordonen. Trots konsensus om vikten av fordonsdata och den övervägande positiva inställningen till delning av fordonsdata har de viktigaste utmaningarna alltid varit hur man motiverar datadelning, hur man skyddar datasäkerhet och integritet, hur man följer EU:s och lokala regelverk och hur affärsmodellerna ser ut. Behovet av metoder och plattformar för att hantera sådana utmaningar är brådskande för att stödja utformningen av nya mobilitetslösningar för hållbara transporter och nya affärspotentialer för att maximera datavärdet.

Projektet fokuserar på datadelning inom fordonsindustrin och genomför först en analys av den senaste datadrivna utvecklingen inom fordons- och transportsektorn. Studien undersöker den kommande datalagen som införts av Europeiska kommissionen och hur den kan påverka det befintliga ekosystemet för data inom fordonsindustrin. Den

framväxande blockkedjetekniken och den snabbt utvecklade tokeniserade ekonomin undersöks utifrån deras potential att stödja datadelning och en datadriven ekonomi. Efter analysen fokuserar projektet på att integrera avancerad krypteringsteknik, blockkedjeteknik och Web 3.0 i en datadelningsplattform för att stödja säker och integritetsskyddande datadelning inom fordonsindustrin. Integritetsskyddad datadelni (Privacy-preserving data sharing, PPDS) föreslås därför med olika arkitekturer som integrerar olika framväxande tekniker för att utforska fordonsdatavärden.

En prototyp har utvecklats och demonstrerats, baserad på avancerad kryptering och blockkedjeteknik. Den föreslagna PPDS-lösningen möjliggör mycket säker och integritetsbevarande datadelning som överensstämmer med GDPR och uppmuntrar dataägare att dela data genom den tokeniserade ekonomin, vilket påskyndar datadriven innovation inom mobilitets- och transportsektorn.

3. Background

Vehicles have become increasingly equipped with advanced connectivity technology including traditional telematics and infotainment systems, as well as the latest advancement in cooperative intelligent transport systems (C-ITS). With the evolution of cellular communications toward 5G and beyond, more data is expected to be available for sharing including various sensor data, driver-related information, as well as infrastructure data perceived by vehicle sensors. Such data has already been used by e.g., original equipment manufacturers (OEMs) to conduct data-driven analysis on vehicle performance and by insurance companies to conduct driver behavior analysis. The increasing amount of data could also generate societal impacts such as improving traffic safety and road maintenance by sharing real-time road and traffic information and contributing to sustainability through eco-driving. The increased amount of data is expected to support even more data-driven services and lead to a huge market potential for automotive data. However, while significant efforts have been made to explore and share vehicle data, challenges remain to be addressed, especially regarding the increased awareness of data ownership, privacy, security, and integrity.

4. Purpose, research questions and method

This project aims at investigating a privacy-preserving data-sharing platform that gives the data owners full control of the usage of vehicle-generated data. Enabled by advanced encryption technologies and supported by blockchain, the platform has the potential to provide a new way for privacy-preserving data sharing that fully complies with GDPR and releases the potential value of vehicle data.

The project aims at answering the following research questions:

- What are the existing data-sharing ecosystems for the vehicle and automotive sectors?
- How will the Data Act affect and transform automotive data sharing?

- How blockchain and Web3.0 may contribute to automotive data sharing?
- Is it feasible to introduce blockchain-based technologies for data sharing?

The project consists of experts within different sectors including automotive data, blockchain, and Web 3.0, and follows closely the latest development within each sector. The project members are active within each sector in participating in conferences and events to follow the latest developments and disseminate the project concepts and results. The project leverages the existing infrastructure and competencies for the conceptualization and prototyping of privacy-preserving data-sharing systems for feasibility study and preparation for further investigation.

5. Objective

The objectives of the project consist of 1) the delivery of a state of the art of automotive data sharing, as well as blockchain and Web 3.0 technologies and their potential to enable privacy-preserving data sharing; 2) the delivery of the core technologies for privacy-preserving data sharing with application programming interfaces (API); and 3) the delivery of an end-to-end prototype for secure vehicle data sharing, where blockchain tokens are investigated.

6. Results and deliverables

6.1. State of the art

6.1.1. Automotive data

Vehicle data is promising to improve traffic safety and many efforts have been made to make Safety Related Traffic Information (SRTI) available. This can be found in the EU ITS Delegated Act 2010/40/EU and No 886/2013. SRTI data includes data related to temporary slippery roads, obstacles on the road, unprotected accident areas, short-term road works, reduced visibility, wrong-way driver, unmanaged blockage of a road, and exceptional weather conditions. Such data are extremely useful to improve traffic safety by warning vehicles ahead of time. Stakeholders from different industries have been working together to investigate methods to share SRTI and the most notable effort is the Data Task Force (DTF). DTF brings together different stakeholders including OEMs, road operators and public authorities from different countries, and service suppliers for a Data for Road Safety ecosystem to demonstrate SRTI data sharing through a pilot project. SRTI information is aggregated by an aggregation partner and is not linked to any individual or personal information, therefore there are no privacy concerns. An aggregation point could be a national partner such as the National Access Point (NAP) regulated by the ITS Delegated Act 2010/40/EU, or private service providers such as Here, Tomtom, etc.

The industry practice for vehicle data access is that OEMs are the gatekeepers, where vehicle data together with certain driver data has been collected by the OEMs with consent from the drivers. Under such conditions, OEMs have the utmost responsibility to manage data security and privacy and enjoy exclusive access to first-hand data. With increased connectivity, the stakeholder ecosystem is expanding to have more connectivity partners such as telecom operators and more service providers that can leverage vehicle data for new services. Since 2017, vehicle data access has been regulated by the EU for repair data and onboard diagnostics (OBD). The improved connectivity e.g., connected vehicles makes much more data available that can be used to create new services.

While the EU is pushing forward data sharing to improve traffic safety such as SRTI, the private sectors work actively to leverage the data value through e.g., the extended vehicle and neutral server. The neutral server dated back to 2016 with the aim of a solution to make vehicle data available for third-party service providers safely and securely. Since then, commercial partners have emerged such as Here, Otonomo, Wejo, and High mobility to provide various vehicle sensor data for service innovation using such a concept. It is by far the practice of OEMs to share data through APIs, however, such a method is simply an API while the standardized definition of vehicle data remains to be investigated such as by the Connected Vehicle Systems Alliance (COVESA)[1]. Despite the legislative efforts and many initiatives that explore automotive data sharing, the data economy driven by automotive data remains rather new and scattered, and the data values are far from being explored.

6.1.2. Data regulations

Being part of the overall data economy, vehicle-generated data is expected to be regulated by the overall data regulations. EU has one of the strongest legal frameworks regarding data privacy, represented by the General Data Protection Regulation (GDPR) and the EU Data Act.

GDPR applies to all organizations in the EU and organizations outside the EU that operate in the EU. GDPR recognizes that personal data is the property of individuals, and they have the right to access, rectify, erase, or restrict the processing of data. As vehicles become connected, many types of data related to vehicles are personalized data and GDPR applies. Under such conditions, organizations that process vehicle data will gain consent from the vehicle owners and need to fully comply with GDPR.

The current data sharing is heavily restricted by GDPR whereby any data that can be used to identify an individual will be removed. In such situations, raw vehicle data is only accessible by OEMs through explicit consent, and only aggregated and processed data is available for sharing based on explicitly defined terms. While GDPR protects privacy and integrity, it poses challenges to data sharing and somehow limits the availability of vehicle data. The practice of GDPR is difficult and OEMs are very careful when sharing such data. Drivers, as data owners, don't have many alternatives to give consent to their

[1] https://www.covesa.global/

vehicles. They don't have enough awareness of how the data has been used either. While data-driven applications have led to economic benefits for different companies, how the drivers as data owners benefit from data usage remains to be investigated. Both private and public stakeholders have been working to explore the value of such data.

In 2020, the EU Commission adopted the European Strategy for data to maximize the potential of industry data and make the EU a leader in a data-driven society. As the latest major legislative initiative, the EU Data Act was proposed in 2022 which sets out the overall principles for data access to connected products by users and third parties. Under the Data Act, users own the rights to access and share data with third parties with compensation and contractual principles for business-to-business data exchange. Rules are also specified for business-to-government data access in exceptional circumstances and switching principles for cloud services.

The Data Act sets horizontal principles for fair data access applying to all digital products. Vehicles as a type of connected products will need to follow the principles that were set by the Data Act, which has direct impacts on the existing in-vehicle data access ecosystems. Vehicle data is generated while drivers are driving the vehicles, and it should be owned by the driver. This essentially moves the data gatekeepers from vehicle manufacturers to the users. However, for vehicles as a traditional consumer product with emerging connectivity, the industry-specified rules to apply the EU Data Act remains to be developed. A vehicle is a complex product with high levels of safety and security, and the automotive sector is very complex with many stakeholders. The EU Data Act will have a significant impact on OEM data ownership, while details on implementation must be clarified and agreed upon. Such implementations need to comply with GDPR and the Data Act, and at the same time accommodate the needs of different stakeholders in the complex automotive ecosystem. While recommendations have been proposed such as by the European Automobile Manufacturers' Association ACEA, the implementation details are still far from being established. It is expected that in the coming years the OEMs will remain as the gatekeepers of vehicle data, while activities on developing solutions to comply with GDPR and Data Act will increase to form new automotive data ecosystems, and to explore more values from vehicle data.

6.1.3. Privacy-preserving technologies

Emerging technologies have been used to enable privacy protection during data sharing, such as encryption, anonymization and pseudonymization, access control, and differential privacy. Notice that many new methods exist for privacy protection, and the following discussion is not exhaustive.

Encryption is the commonly used method to protect data where data is encrypted before being shared. Different encryption methods can be used such as end-to-end (E2E) encryption, fully homomorphic encryption (FHE), and proxy re-encryption (PRE). These methods encrypt data at the source and decrypt data at the destination and keep data encrypted during transmission. This ensures that even the service providers won't be able to access the data. Besides data sharing, FHE also gives the possibility to perform computation on the ciphertext without decryption. This applies to data that holds strong

research and business values but is very sensitive and cannot be shared. PRE allows the delegation of data sharing to a proxy who can convert the ciphertext to another ciphertext under a different public key for sharing purposes. The proxy can only convert, but not decrypt, so it does not affect the privacy of the data.

Anonymization and pseudonymization are other commonly used methods for PPDS by removing or obscuring personally identifiable information (PII) from data or replacing PII with artificial identifiers or pseudonyms to protect privacy. Anonymization methods include randomization to randomly alter the data to obscure PII, generalization to reduce the level of data detail, suppression to remove PII from the data, and so on. Pseudonymization is a (weaker) variant of anonymization whereby PII in data sets are replaced by special purpose identifiers (pseudonyms). With anonymization, it is not possible to link to PII, while with pseudonymization, data sets can be re-identified with the aid of additional information.

Access control is a method to determine who and under what conditions a user is authorized to access the data. This is a critical component in PPDS to allow data access while respecting the privacy of individuals. Access control methods could be identity-based such as by assigning roles and explicit permissions to users based on their responsibilities. It could also be attribute-based where access policies are defined based on the data attributes and the users. Access control can also be combined with encryption for cryptographic access where encryption and digital signatures are used to control the data access.

Differential privacy applies methods to add random noise to the data that can guarantee mathematically that the data being shared cannot be used to re-identify individuals. It can provide high privacy protection while still allowing data to be analyzed and used since the noise is added in a way that makes it cancel out during data sets aggregation. Differential privacy could be global where noise is added globally to all records in the data to protect the privacy of all individuals; and local where noise is added locally to each record to protect the privacy of individual records. This is one of the most effective methods for privacy protection and is widely used in PPDS.

6.1.4. Blockchain, Web 3.0 and the tokenized economy

Blockchain is a decentralized and distributed ledger technology for secure and transparent record-keeping. It is an emerging technology that has been mostly used for cryptocurrency and is the core technology for Web 3.0 where data is owned by generators. It allows multi-parties to access and update the same information without the need for a central authority or trusted third party. It holds the potential for PPDS which allows multiple participants to hold a portion of data, and the data is verified and processed securely and transparently.

While blockchain has been mostly used for cryptocurrency, the application potential to support PPDS remains to be explored. Blockchain usually has limited capacity to handle large amounts of data and the transactions can be slow, which may restrict its usage for real-time applications with large amounts of data sharing. Blockchain ensures secure and

transparent data exchange concerning privacy, but privacy must be handled by other methods such as encryption. PPDS could leverage the advantages of blockchain and many other privacy-preserving technologies for a more secure and efficient PPDS.

Web 3.0 refers to the next-generation Internet where content generators are also content owners in a decentralized, intelligent, and user-centric Internet environment. It is enabled by technologies such as blockchain and distributed computing and allows much greater control and ownership of personal data as digital assets. With Web 3.0, tokenized economy emerges where the economic ownership and value are represented by tokens or digital assets on a blockchain. In such a new economic system, ownership, and assets transfer are managed on a decentralized ledger for secure and transparent transactions. Tokens could also be used for payment and exchange, as traditional currencies. They can be traded on the token market.

The automotive data in Web 3.0 is a digital asset that is owned by vehicle owners. Under the current practice, the data owners could be also the OEMs who have gained consent from the vehicle owners. With the blockchain-based Web 3.0 framework, data owners are motivated to share data with rewards through tokens (i.e., the platform's currency). Such a framework can combine PPDS where tokens are used to represent ownership and data access, and PPDS ensures that the privacy of data is maintained. PPDS in Web 3.0 has the potential to enable a secure and transparent data exchange. With tokens as rewards, data owners are encouraged to share data thus accelerating the circulation of data and data-driven innovation.

A representative product based on Web 3.0 is the DIMO[2] platform which is a decentralized data-driven ecosystem for vehicles. It allows drivers to share data and get rewarded, and developers to build applications on the open network of mobility data. DIMO is a platform that was launched during this project period, which clearly demonstrates the rapid development of emerging methods to explore vehicle data values. While DIMO introduces blockchain tokens for vehicle data sharing, this project aims at more generic solutions for automotive data sharing accommodating the needs of different stakeholders.

6.2. Privacy-preserving data sharing – concept development

PPDS consists of methods that ensure that data is not leaked to any untrusted third parties during the sharing procedure. Through the protection of sensitive information and minimizing the risk of harm to individuals, PPDS enables data sharing to support data-driven research and services while complying with GDPR. PPDS leverages the latest development in privacy-preserving technologies for use case specific solutions. A PPDS concept platform for automotive data sharing is presented. The platform considers both the existing data-sharing practice and the forthcoming EU Data Act that gives more control of data sharing to individual vehicle owners. The architecture and components are described as follows, and a demonstrator system is presented in the next section.

[2] https://dimo.zone/

6.2.1. System architecture

As discussed earlier, the current practice for automotive data sharing is through the OEMs who collect data from vehicles by gaining consent from users. OEMs are then the gatekeepers and share data for different purposes such as to improve traffic safety with SRTI and generate business values with more diverse data streams. We design a PPDS that allows OEMs to share data and data values in a secure and privacy-preserving manner that fully complies with GDPR, thus accelerating the circulation of data and data values.

Figure 1 illustrates the end-to-end architecture of our proposed PPDS under the current automotive data-sharing practices and different scenarios. Several stakeholders are involved in such a PPDS as described below and follow the data-sharing flow.

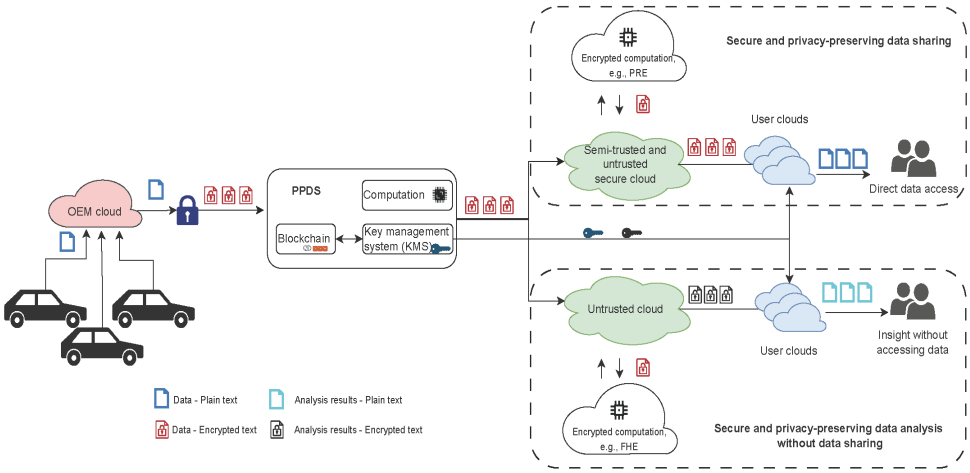


Figure 1 PPDS architecture for vehicle data sharing under existing data usage practices.

- Data generators and owners: The drivers are the data generators and owners. However, under the current practices where drivers give consent to OEMs to collect data, OEMs are then considered as the data owners.
- PPDS platform providers: They are the actors who provide necessary tools including encryption, key management, and blockchain-based methods to allow secure circulation of data and distribution of keys. With the integration of blockchain technologies, PPDS also generates tokens based on data transfer to encourage data sharing.
- Storage: Those could be any cloud storage providers that provide data hosting such as Google, Azure, Amazon, and private cloud. They may be trusted, semi-trusted, or untrusted.
- Computing service providers: Those are actors that provide computational services such as PRE and PHE. Those services require a high level of security and privacy protection and can be computationally demanding.

- Data users/consumers: Those are the organizations that need to conduct research and analysis on automotive data. They could be insurance companies to study general and individual driving behaviors and patterns. They could also be public authorities to investigate the traffic and road conditions. They can even be individual users who want to understand their driving behaviors.

6.2.2. Data vs data value sharing

There can be different ways to allow the circulation of data values, as illustrated in the right part of Figure 1.

Secure and GDPR-compliant data sharing: This method focuses on data sharing. The end user will be able to access the data after decrypting the ciphertext received using private keys. The encryption could be E2E and/or through a proxy. For E2E encryption, the data owners encrypt data at the data source, in this case, the OEM cloud, and take care of the key distributions. In the case that data owners want to skip the key management, they can choose a semi-trusted partner and delegate the data-sharing task to it. For protecting the data, the data owners will not share plain text, but the encrypted text under a public key. The proxy can perform re-encryption using another public key and manage the data sharing with third parties. Under such a case, the data is still E2E encrypted and the proxy shares data without access to the plain text data.

Secure and privacy-preserving data value sharing: This method focuses on information sharing without accessing the raw data. As mentioned earlier, FHE makes it possible to conduct computations on ciphertext without the need to access the original plaintext data. This is important for extremely sensitive data where data sharing is not allowed by the regulations, or data access is not granted by the data owners. While it cannot be shared, such data still have data values that can be used for research and business purposes. FHE, under such situations, allows for data value circulation through sharing only the encrypted ciphertext with no privacy concerns. As illustrated in the lower right part of Figure 1, PHE performs computation on the ciphertext stored on the untrusted cloud and shares the encrypted results to end users. The end users can then decrypt the results with private keys, thus leveraging the data values.

As discussed earlier, with the proposal of the EU Data Act, the role of data owners of the vehicle owners is strengthened and it is possible that vehicle owners, which are drivers, can decide directly which data, to whom, and under what conditions that can be shared. In this case, the data gatekeepers are switched from OEMs to drivers for private vehicles. As illustrated in Figure 2, each vehicle can access the PPDS platform directly and make its data available for third-party usage under strict security and privacy protection. All the data sharing and data value circulation follow the same flow as discussed above. A unique module for the proposed PPDS is the integration of blockchain and Web 3.0, where drivers will receive rewards through tokens as they share data. In other words, the more data the drivers share, the more tokens they will earn. This creates a distributed and much more efficient data marketplace that accelerates the circulation of automotive data and data values.

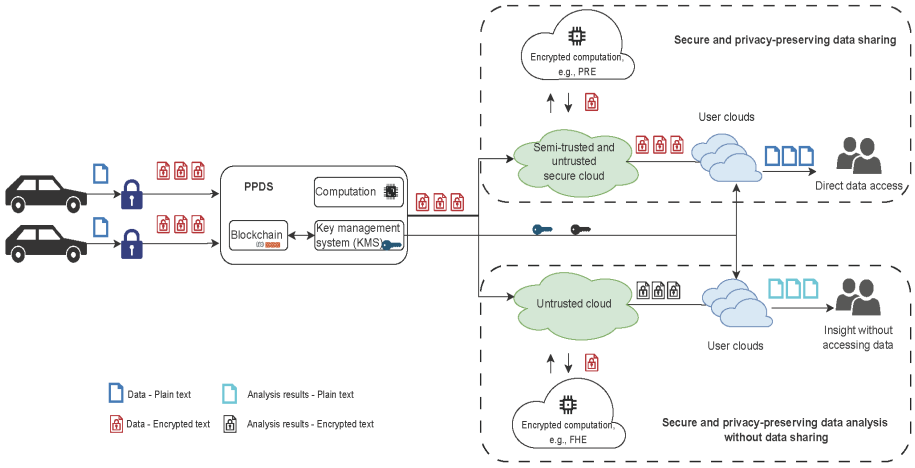


Figure 2 PPDS architecture for automotive data sharing under increased awareness of data privacy and ownership

6.3. PPDS prototype

Following the architecture discussed, a PPDS system prototype has been built for proof-of-concept testing and verification. The prototype is illustrated in Figure 3 and discussed as follows.

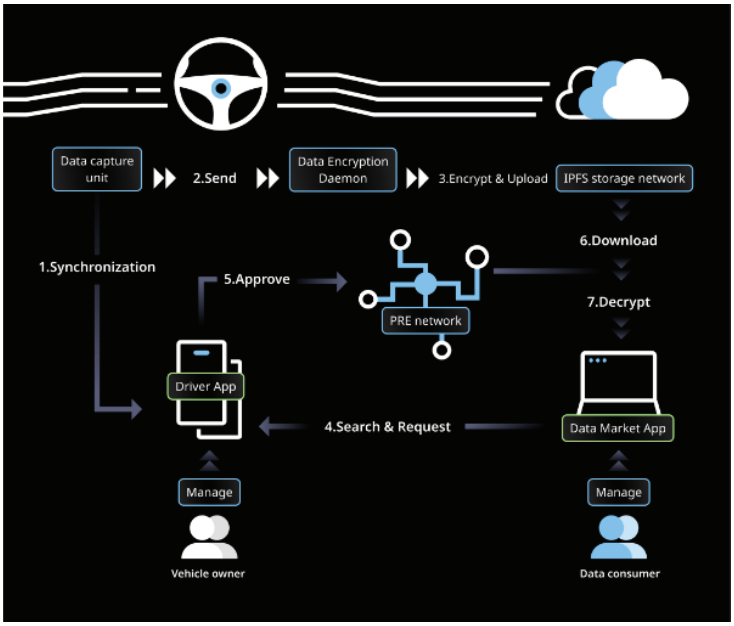


Figure 3 PPDS prototype components and workflows

6.3.1. System components

The prototype consists of main subsystems for continuous data collection and preparation, and for data usage.

The data collection consists of a data capture system, a data encryption daemon module, and data storage.

Data capture system: The data capture unit is the device that accesses the vehicle's onboard diagnostic port and collects in-vehicle signals. The data capture system is provided by Alkit Communications and the data is collected in a file storage folder inside the Linux-based in-vehicle data collection unit (see Figure 4). Collected data currently includes diagnostic data, time-series data from in-vehicle sensors, and various types of status information. The data capture system also supports the collection of other types of data (including audio and video) which is planned in later versions of the prototype PPDS system.

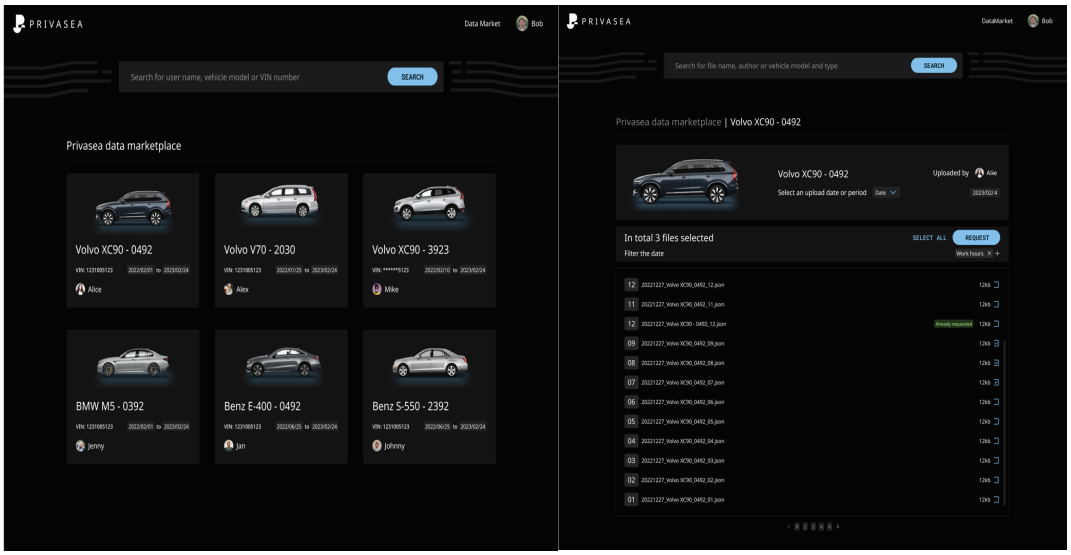
Figure 4 PPDS data collection system

Data Encryption Daemon: This is a service that runs in the in-vehicle Linux system. It encrypts all the data collected by the data capture system and uploads the encrypted data into the PPDS distributed storage network. The storage is based on IPFS (InterPlanetary File System) that is a peer-to-peer hypermedia protocol used for decentralized storage in Web 3.0.

The data usage subsystem takes care of the data request and sharing with the PRE network for ensuring data security. It consists of front-end apps for both the driver and data consumers, as well as PRE network to enable data sharing.

Driver APP: PPDS allows drivers to have full access to their data. Drivers are provided a front-end interface through an App to manage their data such as to grant or reject incoming requests, shown in Figure 5(a).

(a) Driver App



(b) Data Market App

Figure 5 Front-end interfaces to Drivers and data consumers

Data Market APP*:* To allow seamless data sharing, the automotive data market is created and accessed by a data market APP. The APP is a frontend interface for consumers to search and request data access for chosen vehicles, shown in Figure 5(b).

PRE network: The PRE network consists of PRE nodes that conduct proxy re-encryption to enable data sharing. When the driver grants access to data, the PRE node will perform PRE operations to share the data with consumers. As discussed, the PRE has no access to the plain text but can only convert the text to another ciphertext.

Figure 6 The PRE network management portal

6.3.2. Workflow

PPDS enables individual drivers to share data through the data market and drivers are the gatekeepers of the data. Drivers first log into the Driver App to grant access to vehicle data and synchronize the private key from the data capture system. After that, the data capture system starts to collect vehicle data. In the prototype, E2E encryption is used, and once data collection starts, the Data Encryption Daemon will automatically encrypt the data and periodically upload it to the IPFS storage network. Data from all registered vehicles will thus be available in the data market.

On the consumer side, users search the data from the Data Market App, choose the data they are interested in using, and submit requests. As the gatekeeper of their data, data owners review the data access requests and decide if they want to share the data. If data access is granted, the PRE network will take care of the data sharing. Notice that user data is encrypted from the vehicle side and the PRE network has no access to the plain text. PRE nodes perform proxy re-encryption and share the ciphertext with the authorized data users and the data is decrypted on the consumer side.

As mentioned in the PPDS design, different business models can be used for rewarding data sharing. In addition to traditional business models, a tokenized model is embedded in our design, and tokens are generated automatically when drivers grant data access.

6.4. Summary

The project achieves its goals of the delivery of state-of-the-art of automotive data sharing, Data Act, and privacy-preserving methods for automotive data sharing including blockchain and Web 3.0. The project delivers a prototype of a privacy-preserving data-sharing system that consists of a data capture system by Alkit Communications AB, a data encryption daemon module by Privasea AB, and data storage. Demo apps for drivers to manage their data access are also prototyped.

The project demonstrates a data-sharing solution for exploring data values. The transport solutions enabled by data-driven methods will contribute to the FFI impacts for developing safe, equal, and efficient mobility solutions. The exploration and integration of blockchain and tokenized economy motivates data owners to share data, thus enabling data-driven mobility solutions that contributes to FFI for sustainable mobility solutions with high acceptance by the users and society. Data sharing requires an ecosystem, especially for the automotive sector. Though it is too early, the project leverages blockchain solutions and the latest privacy-preserving technologies for an innovative platform that has the potential to accelerate vehicle data sharing, which contributes to FFI on developing new skills, infrastructure, policy, and regulation, as well as business models on data sharing, thus enabling innovative solutions for road transport.

7. Dissemination and publications

7.1. Dissemination

How are the project results planned to be used and disseminated?	Mark with X	Comment
Increase knowledge in the field	X	Increase the knowledge on automotive data sharing, regulation, as well as privacy-preserving technologies including Web 3.0.
Be passed on to other advanced technological development projects	X	Different privacy-preserving technologies have been used in projects by the participating companies and blockchain-based methods are under further development.

Be passed on to product development projects	X	Privacy-preserving technologies such as encryption, and access control are used for data collection and sharing product.
Introduced on the market		The market introduction needs further investigation partially to follow the EU Data Act, and partially to create business models based on blockchain and tokenized economy.
Used in investigations / regulatory / licensing / political decisions		Too early to support such activities.

7.2.

7.3. Publications

Lei Chen, David Jiao, Mathias Johanson, Privacy-preserving data sharing for automotive applications, the 29th ITS World Congress, Suzhou, 2023.

8. Conclusions and future research

Vehicles are increasingly connected and automated, and data generated from the vehicles hold value for generating new business values and societal impacts. While broadly accepted standards to define vehicle data and interoperable methods for seamlessly circuiting the data are still missing, stakeholders are working together to address the challenges from different perspectives. This project proposes data-sharing architectures with a focus on privacy-preserving data sharing (PPDS). With PPDS, the data owners have full control of the data and grant access to vehicle data to whom they are willing to. PPDS enables a paradigm shift in data ownership. It aligns with the EU Data Act and fully complies with GDPR while encouraging data sharing through innovative business models such as the tokenized economy. This gives users (i.e. drivers) incentives to grant access to data in a controlled and trusted way.

A proof-of-concept PPDS prototype system has been built and presented. Testing and validation are ongoing with test vehicles and preparations to invite private vehicle drivers are in progress in parallel.

Transport data is a key pillar in future digital transport infrastructure and automotive data represents a key part of future transport data where many challenges remain regarding data collection, management, sharing, and monetization.

- The impact of the EU Data Act on vehicle data remains heavily discussed and a standardized definition and interoperable methods of data representation and sharing remain to be developed. Close observation and active contribution to the Data Act from the automotive industry are required.
- Innovative business models are important to encourage data and value circulation. Under the current data-sharing practice, it is about making it easier to allow third parties to access data through API. There have been efforts regarding this while much remains to be done to fully explore the data value. Potentially as a future practice, drivers as data owners will decide about the data sharing directly from the vehicle. This will liberate the data under the condition that security and privacy will be addressed properly. Blockchain-based Web 3.0 has been used to address this, as is being done in this project, and more efforts are expected to emerge.
- The current data access is done through e.g. extended vehicle, CAN bus, and the Android automotive with some vehicle signals available, while a standardized and interoperable representation of vehicle signals remains to be developed. Industry collaborations and standardization efforts are needed at the international level.
- Privacy and security remain the key concern for data sharing, and PPDS will require further development including the integration of emerging technologies such as encryption and blockchain. This is a general topic and automotive data sharing requires tailored solutions.
- Web 3.0 and tokenized economy enjoy rapid development while their application in the automotive industry is new. Much work is required to observe the trend, technologies, risks, and regulations for exploring the potential benefits while eliminating the potential risks.

9. Participating parties and contact persons

RISE Research Institutes of Sweden, Lei Chen, lei.chen@ri.se

Alkit Communications AB, Mathias Johanson, mathias@alkit.se

Privasea AB, David Jiao, david@privasea.tech