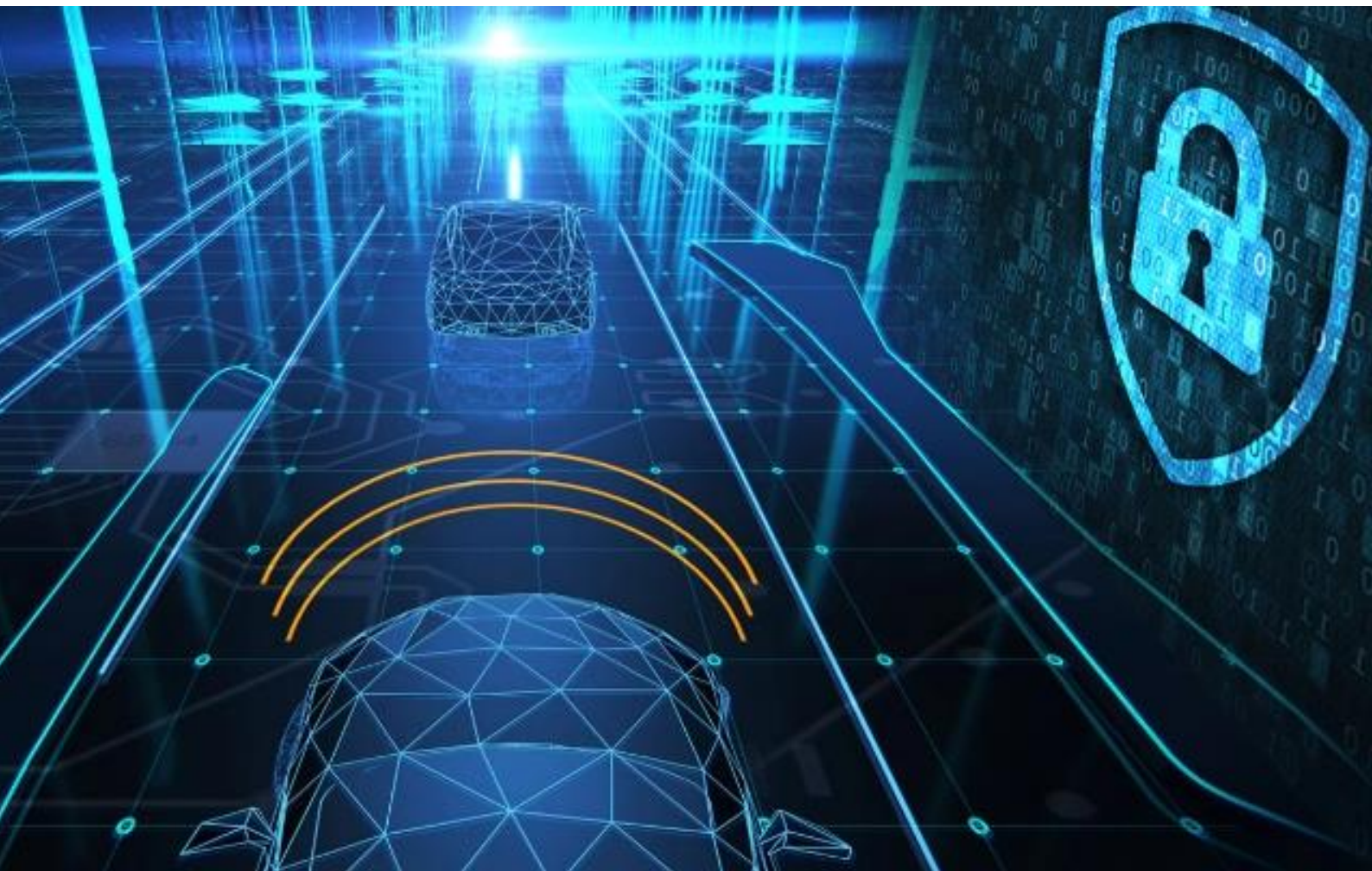


Demonstrator of Services Using Integrated CPP and Insurance Data

Public Deliverable D6.5



December 2022



This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 871477

Foreword

Welcome to our smashHit Demonstrator of Services Using Integrated CPP and Insurance Data. From the very beginning of the project, we were absolutely convinced that the growing Data Economy has to become more attractive for its key stakeholders (data subjects, data providers and data controllers) to overcome existing barriers, especially the complicated and time-consuming consent/contract processes, hindering the build-up of innovative services using data from multiple sources.

With the growing ability of Consumer Products (CP, such as cars, smart devices, etc.) to generate, gather and share data with third parties among different data-sharing platforms, there will be a general need for flexible and easily manageable procedures to handle data subject's consent and legal rules, to achieve effective and traceable contracting. The complexities of the General Data Protection Regulation (GDPR), for example, possess some challenges and require complex mechanisms to obtain, record and manage consent. Also, data subjects are afraid about improper use of their data. The combination of understanding and relating to the value proposition, consumer trust, and complex consent processes, results in a low opt-in rate for connected product data exchange (e.g. data from cars) and prevents the creation of innovative services (e.g. connected vehicle insurance programs, or smart city solutions).



Thus, we have conceptualised the smashHit system solution as a trusted and secure reference Framework, integrating privacy-by-design, to simplify the consent/contract process, as well as to enable consent/contract tracing and sharing among multiple data platforms. In addition, smashHit will offer solutions to identify data misuse as well as to support stakeholders in the creation of legally binding contracts.

All along, we have followed the maxim to think about the needs of data subjects and data customers, but also to convince CP manufacturers (e.g. car makers) to open up their products, by designing a convincing trustworthy ecosystem.

During the project lifetime we have finalized the smashHit system concept, its detailed specification and development by our software and RTD development partners and created a working prototype capable of scale. Several public presentations of our smashHit system concept and results have been made (see smashHit project website).

This public report covers the Demonstrator of Services Using Integrated CPP and Insurance Data (smashHit Business Case 1).

If you are curious about how all that is made possible, just continue on the following pages, enjoy the reading, and please contact us with your feedback or questions!

-  smashHit support email: info@smashhit.eu
-  smashHit project website: <https://smashhit.eu>

Executive Summary

The objective of smashHit is to assure trusted and secure sharing of data streams from both personal and industrial platforms, needed to build sectorial and cross-sectorial services, by establishing a Framework for processing of data subject consent and legal rules and effective contracting, as well as joint security and privacy preserving mechanisms. The vision of smashHit is to overcome obstacles in the rapidly growing Data Economy which is characterized by heterogeneous technical designs and proprietary implementations, locking business opportunities due to the inconsistent consent and legal rules among different data-sharing platforms actors and operators. The Framework will provide methods and tools, such as the smashHit Platform.

This document, which comprises the Demonstrator of the smashHit Business Case 1 is structured as follows:

1	Demonstrator of UC1.1 - LexisNexis Consent Management Platform	5
1.1	Demonstration Part 1 – Consent Grant.....	5
2	Demonstrator of UC1.2 - Vehicle (Volkswagen) Connectivity and Data Traceability..	9
2.1	Vehicle Connectivity	9
2.1.1	Vehicle Data Sharing.....	9
2.1.2	Consent Management in the Vehicle	11
2.2	Data Traceability	12
2.2.1	Traceability	12
2.2.2	Watermarking	15
3	Glossary.....	18

List of Figures

Figure 1: Screenshot of the simulated insurers App.....	5
Figure 2: The LexisNexis CMP showing consent has been transferred from the App	6
Figure 3: Screenshot showing data is flowing from the VW CarNeo system	6
Figure 4: Screenshot of the smashHit user log-in screen.....	6
Figure 5: Screenshot of the user consents.....	7
Figure 6: The smashHit User Interface showing consent has been revoked	7
Figure 7: Pop-Up window in the smashHit User Interface requesting confirmation of Opt-Out	8
Figure 8: Screenshot showing data from CarNeo stops flowing after consent withdrawal	8
Figure 9: Detailed illustration of data collection and bundling of different data requests (projects) from multiple smashHit partners on the same vehicle	9
Figure 10: CarNEO as in-car App (photo of the infotainment system in the test vehicle, CarNEO is the prototype in-car app for managing the consents and CarNEO dev Console is for debugging and logs viewing)	11
Figure 11: CarNEO as in-car App – List of active consents, with the possibility to revoke them	11
Figure 12: The endpoints provided by the traceability module and used by CarNEO on OEM side to enable the data use traceability	12
Figure 13: Consent template ready for requesting the user consent. The agents listed should be able to use the data following the purpose description.....	13
Figure 14: Consent request granted by the Data owner: all applications in the consent (VW and Traceability App) can now use the data.	13
Figure 15: Data owner can see the <i>traceability information</i> related to his/her consent	14
Figure 16: Traceability data related to the granted consent (as seen in the Traceability Manager UI).	14
Figure 17: Table of database showing the identifier (URI) of each actor. In the previous screen, VW is sender and Traceability App is receiver.....	15
Figure 18: Trajectories used in the scenario	16
Figure 19: Consents granted and trajectories shared.....	16
Figure 20: Consent granted for company 1 (LUH) on the top, company 2 (UBO) on the bottom	17
Figure 21: Leaked data discovery and leakage check.....	17

1 Demonstrator of UC1.1 - LexisNexis Consent Management Platform

This demonstrator has also been compiled in a video. It can be accessed online at:

<https://vimeo.com/785239596/af16603a53>

The main objectives for the demonstrator are:

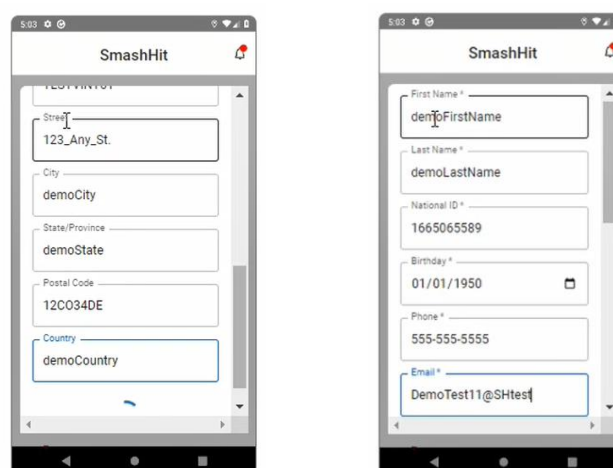
- Demonstrate how the key elements can communicate and create a legitimate information flow involving:
 - Citizen
 - Connected Vehicle
 - Consent Management Platform and Insurer
 - smashHit Platform
- Demonstrate how the user interface will give the Citizen transparency and control of the consent process.
- Demonstrate how the citizen has flexibility of exactly where and how he/she can grant and withdraw consent for data sharing.

The demonstrator shows the interaction between the actors involved in the business case - namely the consumer, the vehicle manufacturer (VW), the data processor (LexisNexis) and the insurer (fictional) – and smashHit. The final prototype included an integration between the LexisNexis CMP and smashHit, the VW Data Platform (CarNeo) and smashHit, and the VW Data Platform (CarNeo) with the LexisNexis Telematics Platform. All of these elements are included in the demonstrator.

At a high level, it is possible to demonstrate the interaction with smashHit and the various scenarios and outcomes that would be achieved for a citizen seeking to manage a consent process for vehicle insurance

1.1 Demonstration Part 1 – Consent Grant

The demonstration starts with a fictional consumer requesting a new UBI policy from a fictional insurer. In the demonstration, this is done via a simulated insurer App.



The image displays two side-by-side screenshots of a mobile application interface titled "SmashHit". Both screens show a registration form for a fictional insurer.

The left screenshot shows the address section of the form with the following fields and placeholder text:

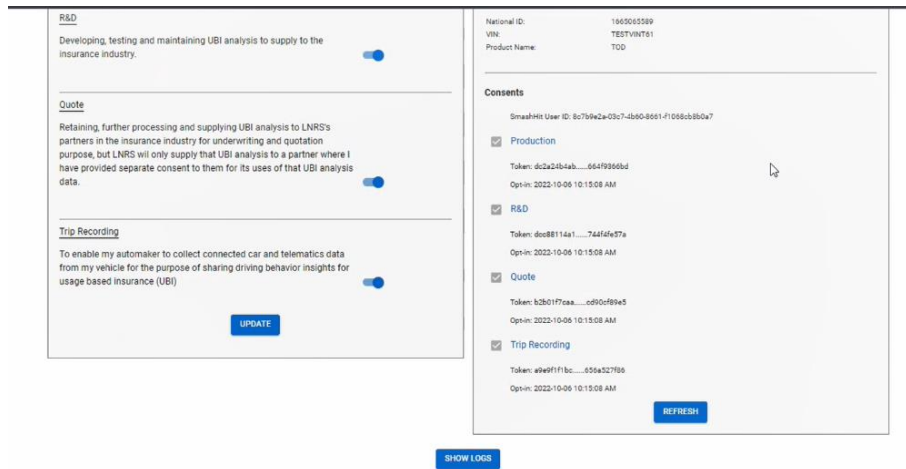
- Street: 123_Any_St.
- City: demoCity
- State/Province: demoState
- Postal Code: 12C034DE
- Country: demoCountry

The right screenshot shows the personal information section of the form with the following fields and placeholder text:

- First Name: demoFirstName
- Last Name: demoLastName
- National ID: 1665065589
- Birthday: 01/01/1950
- Phone: 555-555-5555
- Email: DemoTest11@SHtest

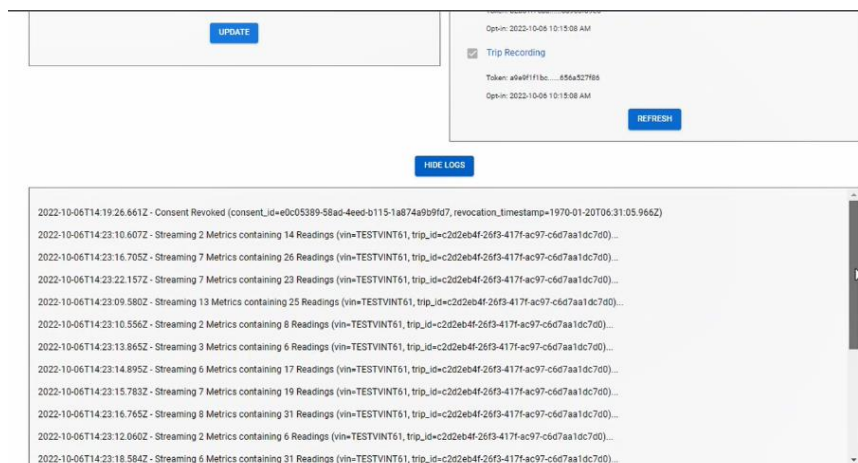
Figure 1: Screenshot of the simulated insurers App

The consumer's consent to share driving data for the insurance use case is captured by the LexisNexis CMP and shown in the following screen:



Information is then sent to the SmashHit system where the consent is verified, and a unique certification token is returned to the appropriate partners. In this case, the OEM trip recording consent is sent to Volkswagen indicating that trip data for this vehicle may be collected and shared for the purpose of usage-based insurance.

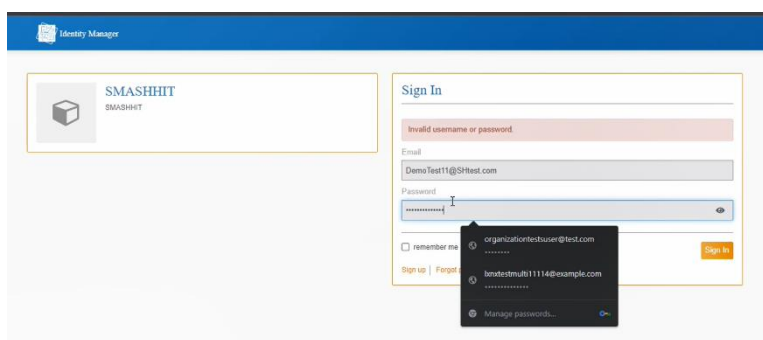
Figure 2: The LexisNexis CMP showing consent has been transferred from the App



The sharing of trip data between VW and LexisNexis is then demonstrated via the LexisNexis user interface. The data flowing from the vehicle to the LexisNexis system is seen on the screen at the bottom of the diagram.

This data would be processed in line with the consent given to provide Insurance Services products to the insurer.

Figure 3: Screenshot showing data is flowing from the VW CarNeo system



The consumer can now log into the SmashHit system as a data owner to view and manage consents he/she they has granted.

Figure 4: Screenshot of the smashHit user log-in screen

This screen shows the consents granted by the consumer via the simulated insurer App, as now recorded in smashHit.

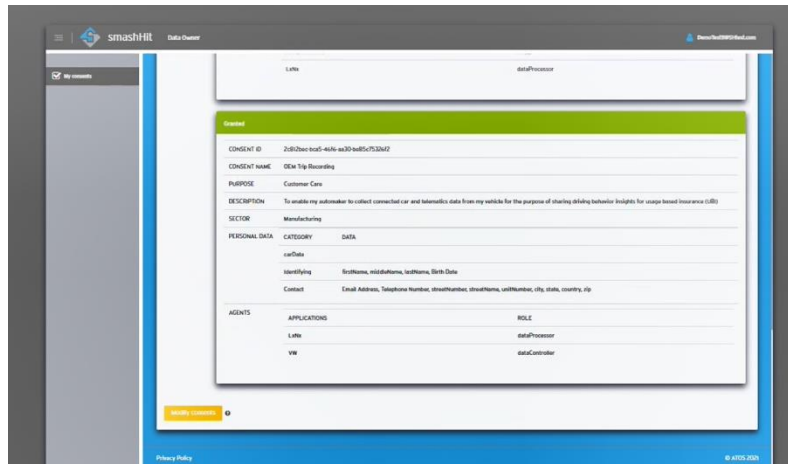


Figure 5: Screenshot of the user consents

Although the consent was initially granted via an insurer App, it can easily be withdrawn by the consumer via the smashHit user interface.

This consumer has decided to revoke its consent for Trip Recording. To update, the consumer selects modify consents, scrolls to the consent he/she wishes to revoke and selects revoke consent.

This action creates a new consent token in smashHit which is shared with the relevant parties – LexisNexis and VW.

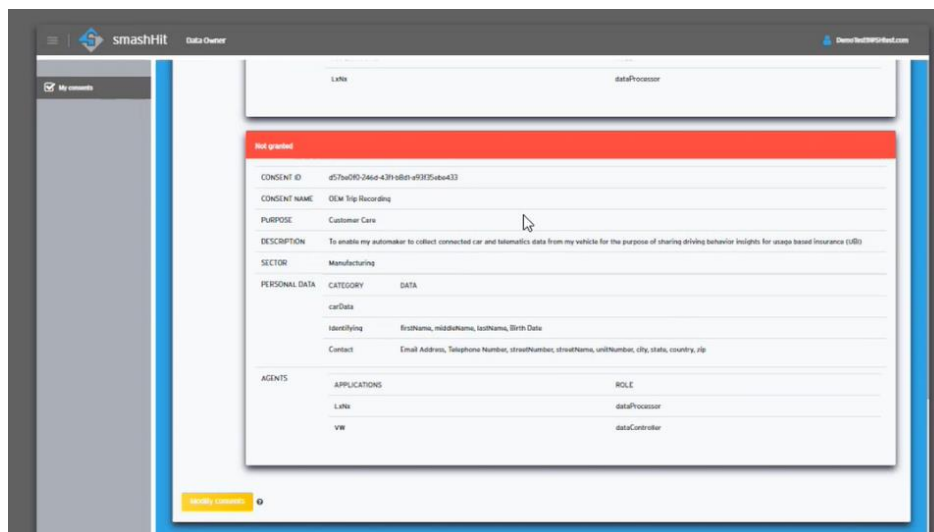


Figure 6: The smashHit User Interface showing consent has been revoked
When changing a consent, the user is requested to confirm the change.

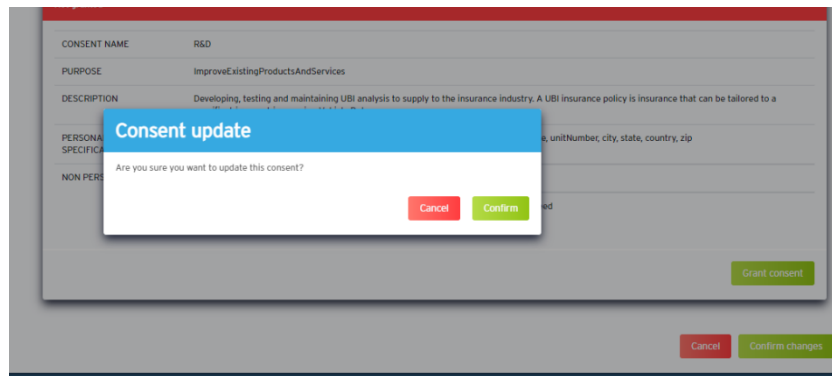


Figure 7: Pop-Up window in the smashHit User Interface requesting confirmation of Opt-Out

Returning to the LexisNexis user interface, the demonstrator shows that the consent update has been pushed to the consent management platform, which now correctly displays the Trip Recording consent in an opt-out status.

But not only does the demonstrator show the change of consent status to opt-out, but the screen also shows and demonstrates that the opt-out is successfully actioned, and the data has stopped flowing between the VW and LexisNexis systems. A notice appears in the data stream indicating that consent has been withdrawn.

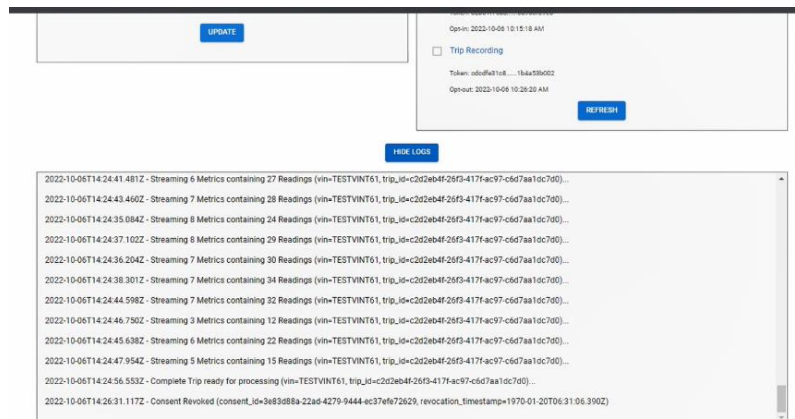


Figure 8: Screenshot showing data from CarNeo stops flowing after consent withdrawal

To summarize, the smashHit demonstrator for this use case shows that smashHit brings the following benefits to the consent process:

- A single-click consent experience that enables the service the consumer is purchasing
- A single-click consent withdrawal process which stops data flow immediately
- A consumer can grant and withdraw consent anywhere:
 - On a website or mobile App
 - From the car
 - With their insurer

And the consumer has complete transparency and control of data sharing.

2 Demonstrator of UC1.2 - Vehicle (Volkswagen) Connectivity and Data Traceability

UC1.2 demonstrator videos can be accessed online at:

<https://www.youtube.com/watch?v=awjAyXuopBI>

<https://www.youtube.com/watch?v=HZK7XXNlXn4>

Further details can be found in the following text.

2.1 Vehicle Connectivity

The vehicle connectivity and configuration work, as part of the full prototype development, focuses on supporting consent management and GDPR-compliant data sharing activities on the OEM side (Volkswagen in particular) and inside the vehicle including data use traceability as a basis for several business use cases.

This requires the capability to share relevant driving behaviour related sensor data either as a data stream (in near real-time fashion) or in a batch mode after each trip. Furthermore, and in order to ensure GDPR-compliant sharing of the data, an in-car application with a user interface has been developed to enable the driver to view and manage all active consents directly in the car including the possibility to view active consents, see which data is being shared and the ability to revoke an active consent directly in the in-car app.

A demonstration of these functionalities and their in-car interface is given in the video provided in previous section (within UC1.1).

2.1.1 Vehicle Data Sharing

Within smashHit, the OEM vehicle data interface (CarNEO) allows for the collection of data for multiple separate data collection use cases, so-called projects, on the same vehicles. For each project, the consent list is checked against the smashHit consent APIs prior to any data transfer. Therefore, all actors in the consortium can access vehicle data using a unified consent management system.

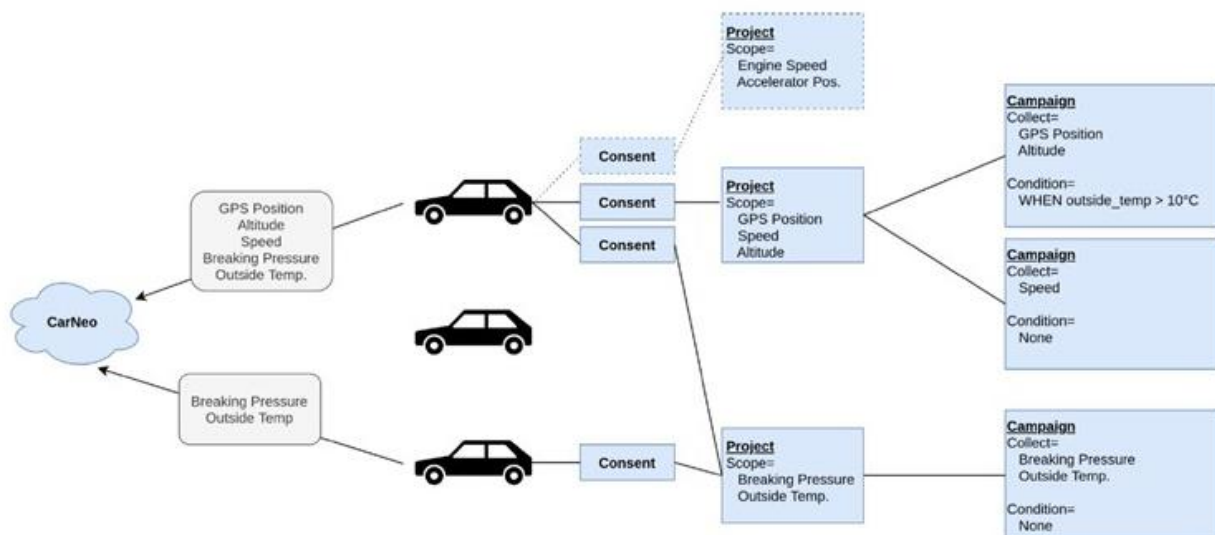


Figure 9: Detailed illustration of data collection and bundling of different data requests (projects) from multiple smashHit partners on the same vehicle

The data flow depicted in Figure 9 illustrates how multiple consent use cases, which use the smashHit platform, can be realized on a group of vehicles. Each vehicle executes a vehicle app that is installed to the infotainment unit. From this vehicle client, several vehicle sensors and APIs are probed to determine the capability map of the vehicle. Based on this capability map, such use cases may choose if a given sensor is required or optional for a given data collection campaign. The vehicle client aggregates the requested metrics such that data is collected and transmitted only once, even if it is requested by multiple applications.

Vehicle sensors requirements may further contain logic conditions. For example, a data collection campaign may depend on a certain value of the ambient temperature ($>10^{\circ}\text{C}$). Unless this condition is met, the vehicle client does not collect and transmit the sensor data to the data campaign. The data collection conditions may be used to define geofencing and behaviour specific activations, e.g., a high braking pressure, etc.

2.1.1.1 Vehicle Sensor Data

As part of this full prototype integration, the vehicle metrics shown in the following table are made accessible to third parties via the current CarNEO prototype.

Table 1: Vehicle metrics currently supported by CarNEO

Sensor data
Steering Wheel Angle
Accelerator Position
Front Wheel Angle
Vehicle Type
GPS Position
Brake Pressure
Yaw Rate
Lateral Acceleration
Longitudinal Accel.
Heading
Vehicle Speed
Engine Speed
Odometer
Altitude

2.1.1.2 Data Subscription Modes

For making the mentioned vehicle data available to third parties, the vehicle interface distinguishes between two different modes: a trip files mode and a streaming mode. During a drive with activated trip files mode, the vehicle collects the data and sends it regularly to the backend. After a signal, that indicates the end of a trip, the backend puts all the trip data together and creates a single trip file, which can then be downloaded by the third party. Using the second mode, the streaming mode, the vehicle sends new data with a frequency of 1Hz to a receiver. In contrast to

the trip file mode, a trip file is not being generated after the vehicle finishes a drive in the streaming mode. Both modes aim to enable third parties to use vehicle data in a vast variety of use cases.

2.1.2 Consent Management in the Vehicle

For managing the consent inside the vehicle, a simple infotainment UI was developed. It is shown in Figure 10 and Figure 11. The infotainment app shows the active consent of the user and it is possible to revoke the consent via the application.



Figure 10: CarNEO as in-car App (photo of the infotainment system in the test vehicle, CarNEO is the prototype in-car app for managing the consents and CarNEO dev Console is for debugging and logs viewing)

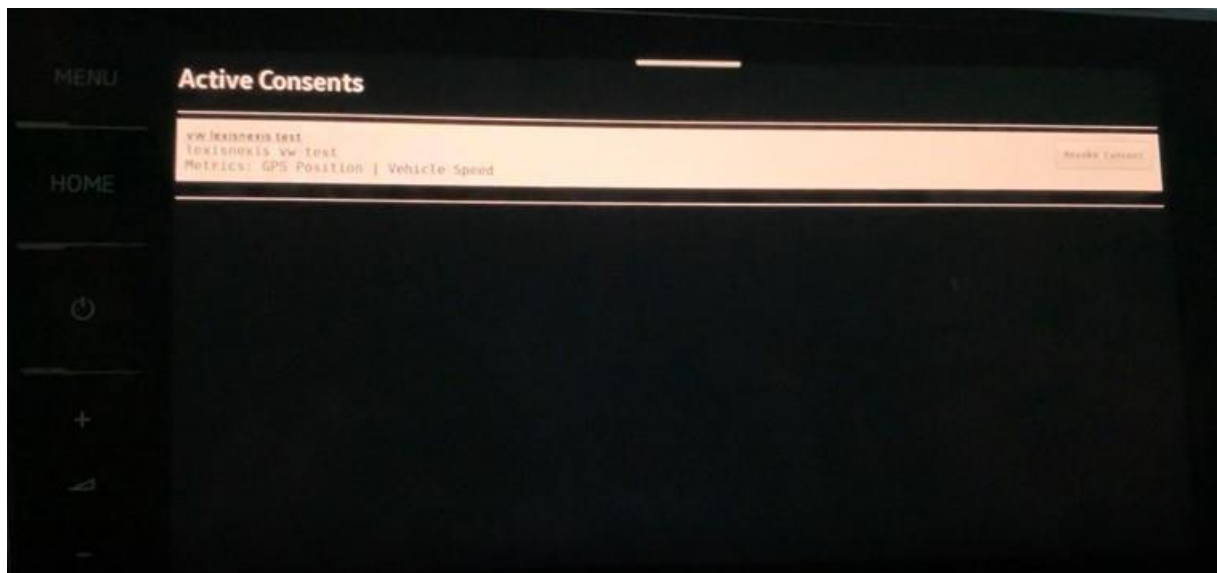


Figure 11: CarNEO as in-car App – List of active consents, with the possibility to revoke them

2.2 Data Traceability

2.2.1 Traceability

The traceability of data shared between partners in smashHit is performed using the traceability module components and their REST API endpoints (Figure 12). The process starts with a consent request to the user from which the data will be collected (Figure 14) inserting as agents the list of partners interested in that data. The consent request should formally meet some smashHit requirements, so the consent template is generated from the smashHit user interface (Figure 13) and used for the request. After the request is granted (Figure 15), the data sharing process can take place. Any time a data under a given consent is registered, transferred or received, the operation is tracked and the logs are stored in a centralized database (Figure 17). The data subject providing the data, can then get the trace based on the consent through the smashHit's user interface (Figure 16).

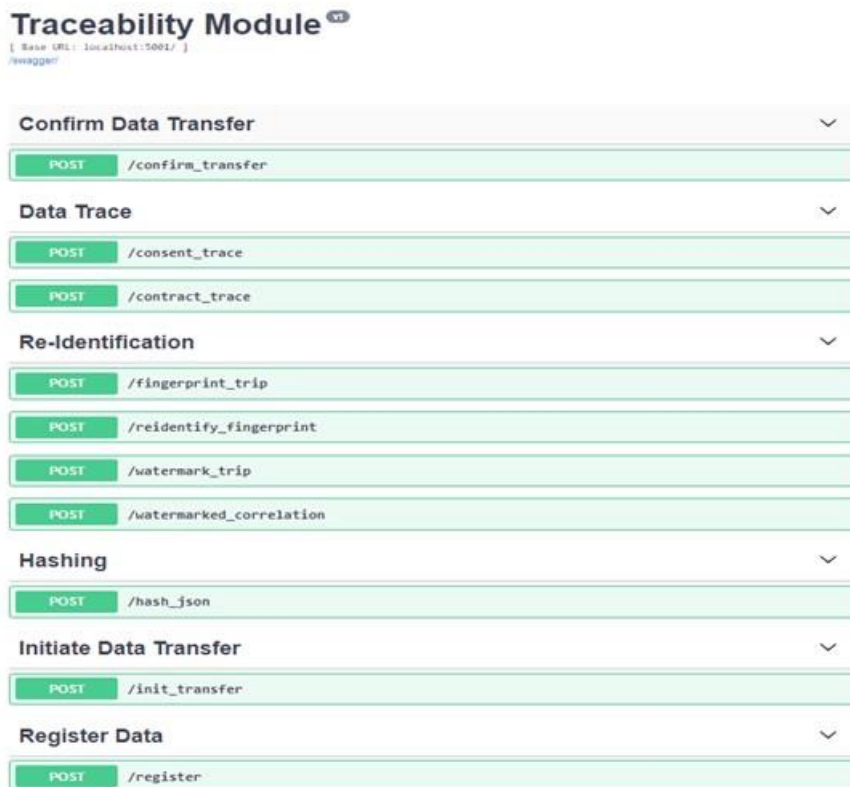
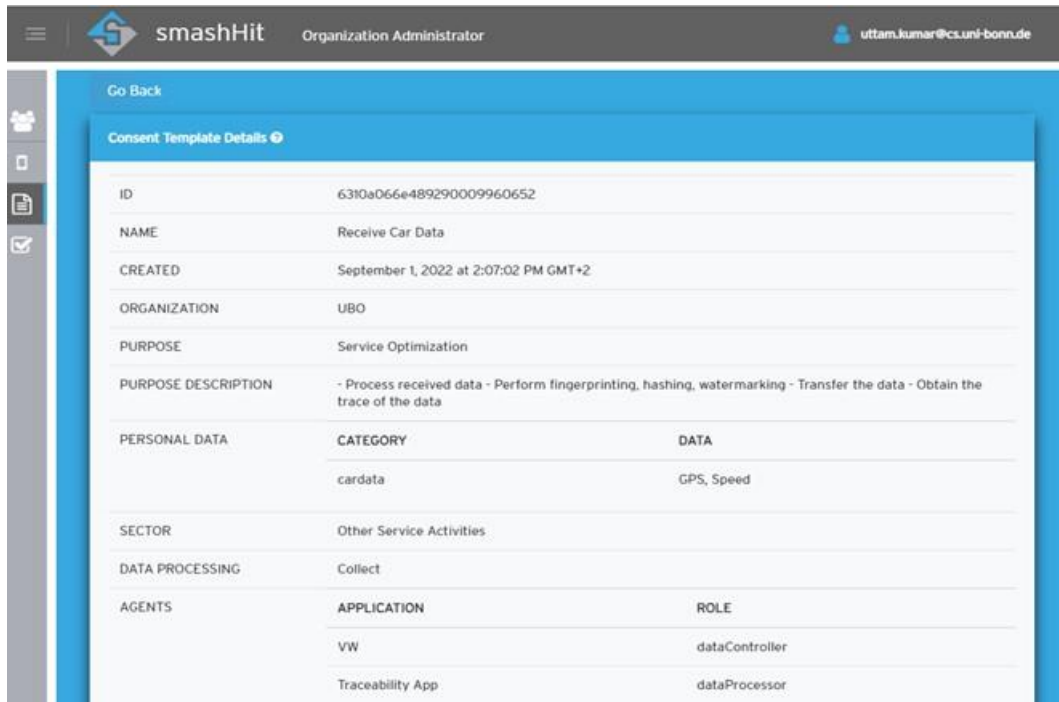


Figure 12: The endpoints provided by the traceability module and used by CarNEO on OEM side to enable the data use traceability

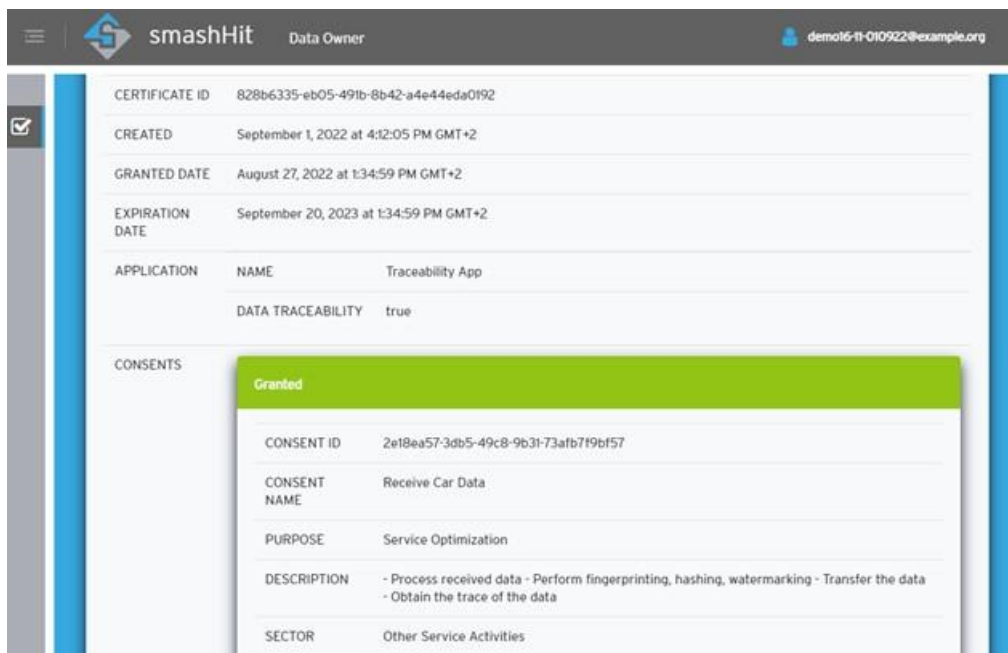


Go Back

Consent Template Details

ID	6310a066e489290009960652	
NAME	Receive Car Data	
CREATED	September 1, 2022 at 2:07:02 PM GMT+2	
ORGANIZATION	UBO	
PURPOSE	Service Optimization	
PURPOSE DESCRIPTION	- Process received data - Perform fingerprinting, hashing, watermarking - Transfer the data - Obtain the trace of the data	
PERSONAL DATA	CATEGORY	DATA
	cardata	GPS, Speed
SECTOR	Other Service Activities	
DATA PROCESSING	Collect	
AGENTS	APPLICATION	ROLE
	VW	dataController
	Traceability App	dataProcessor

Figure 13: Consent template ready for requesting the user consent. The agents listed should be able to use the data following the purpose description



Consent Request Details

CERTIFICATE ID	828b6335-eb05-491b-8b42-a4e44da0192	
CREATED	September 1, 2022 at 4:12:05 PM GMT+2	
GRANTED DATE	August 27, 2022 at 1:34:59 PM GMT+2	
EXPIRATION DATE	September 20, 2023 at 1:34:59 PM GMT+2	
APPLICATION	NAME	Traceability App
	DATA TRACEABILITY	true

CONSENTS

Granted

CONSENT ID	2e18ea57-3db5-49c8-9b31-73afb719bf57	
CONSENT NAME	Receive Car Data	
PURPOSE	Service Optimization	
DESCRIPTION	- Process received data - Perform fingerprinting, hashing, watermarking - Transfer the data - Obtain the trace of the data	
SECTOR	Other Service Activities	

Figure 14: Consent request granted by the Data owner: all applications in the consent (VW and Traceability App) can now use the data.

Granted		
CONSENT ID	2e18ea57-3db5-49c8-9b31-73afb719bf57	
CONSENT NAME	Receive Car Data	
PURPOSE	Service Optimization	
DESCRIPTION	- Process received data - Perform fingerprinting, hashing, watermarking - Transfer the data - Obtain the trace of the data	
SECTOR	Other Service Activities	
PERSONAL DATA	CATEGORY	DATA
	cardata	GPS, Speed
AGENTS	APPLICATIONS	ROLE
	VW	dataController
	Traceability App	dataProcessor
See traceability information		

Figure 15: Data owner can see the *traceability information* related to his/her consent

smashHit

Data Owner

demo16-ff-OIO922@example.org

My consents

CONSENT ID

2e18ea57-3db5-49c8-9b31-73afb719bf57

CONSENT NAME

Receive Car Data

Traceability data.

receiver_id	*sender_id*	*signature_of_receiver*	*signature_of_sender*	*transfer_date_time*	*uniform_resoun
7596a22-40a2f1ed-8cdc-4122cc65b5e4	a1870f6-40a2f1ed-8cdc-4122cc65b5e4	13a74c2d5d7da8ca0b6e880d946299f01c95c05565d08046	3e02ef7efce9ce409eaa7fc32ec72132e860e8ae418ebf	022-09-30 09:56:35.416049	22a3dbc-40a4-f1-00163e38af9c

Close

VW

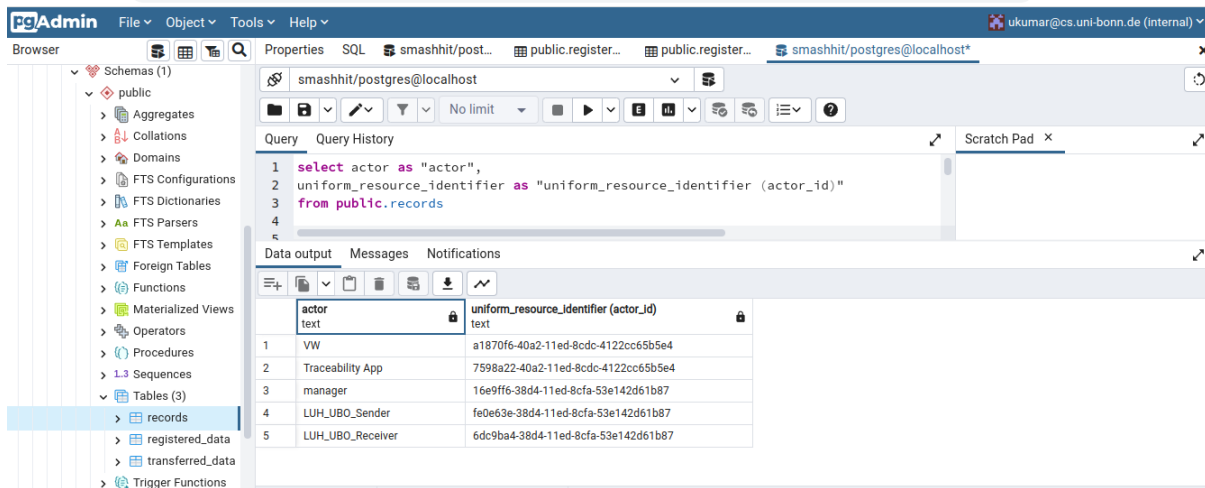
dataController

Traceability App

dataProcessor

See traceability information

Figure 16: Traceability data related to the granted consent (as seen in the Traceability Manager UI).



The screenshot shows the PgAdmin interface with a SQL query executed against the 'smashhit/postgres@localhost' database. The query is:

```
1 select actor as "actor",
2 uniform_resource_identifier as "uniform_resource_identifier (actor_id)"
3 from public.records
4
```

The results are displayed in a table with the following data:

	actor	uniform_resource_identifier (actor_id)
1	VW	a1870f6-40a2-11ed-8cdc-4122cc65b5e4
2	Traceability App	7598a22-40a2-11ed-8cdc-4122cc65b5e4
3	manager	16e9ff6-38d4-11ed-8cfa-53e142d61b87
4	LUH_UBO_Sender	fe0e63e-38d4-11ed-8cfa-53e142d61b87
5	LUH_UBO_Receiver	6dc9ba4-38d4-11ed-8cfa-53e142d61b87

Figure 17: Table of database showing the identifier (URI) of each actor. In the previous screen, VW is sender and Traceability App is receiver

2.2.2 Watermarking

For the watermarking demonstrator, we provide a video (<https://www.youtube.com/watch?v=awjAyXuopBI>) showing in detail the different phases of a GPS trajectory watermarking process, namely:

- Initial GPS trajectory
- Insertion of watermark
- Modification of the watermarked trajectory: In the video, the term “attack” is employed instead of the term “modification” but an attack is just a specific case of modification where the modification of the data is made by a malicious entity (attacker) to hide the origin of this data. Hiding the origin could allow the attacker to redistribute the data.
- Trajectory re-identification using correlation computation

To try the steps presented in the video, we provide the following link <http://watermark.smash-hit.l3s.uni-hannover.de/>.

A video presenting a user story is available at this link - <https://www.youtube.com/watch?v=HZK7XXNlXn4>. The video shows the importance of watermarking in the context of data sharing.

We consider one user and two companies (LUH and UBO) willing to use the trajectories generated by that user. Figure 18 shows the 19 watermarked to be used.

- Trajectory A: watermarked trajectory of **data subject** for company 1
- Trajectory B: watermarked trajectory of **data subject** for company 2

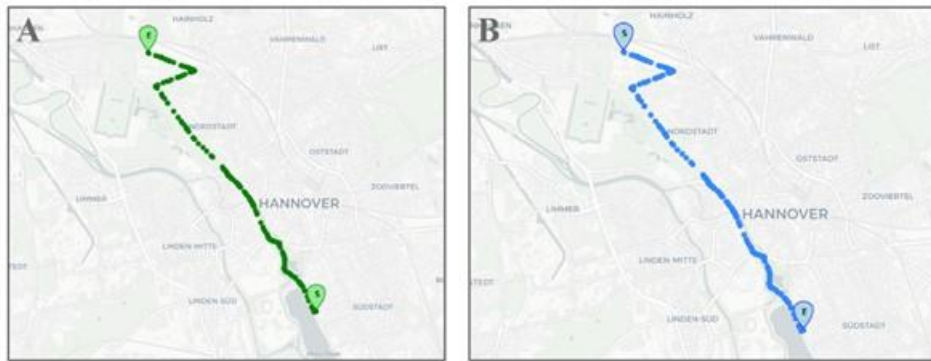


Figure 18: Trajectories used in the scenario

A first consent with ID 303e7bc1-5813-40f3-a92a-6b79b421877f, including company 1 (LUH) is granted by the data subject. A second consent with ID 97c8f942-f37e-4a2b-9ab5-34c792692b7a, including company 2 (UBO) is also granted by the data subject.

While driving from home to the office, the raw trajectory is generated by the data subject. Using a secret, the so-called watermark, this trajectory is watermarked and forwarded to Company 1. A secret or watermark here represents a piece of information that is inserted in a data to be able to recognize that data later on. Using another secret, the same raw trajectory is watermarked and forwarded to Company 2.

This process is summarized in Figure 19.

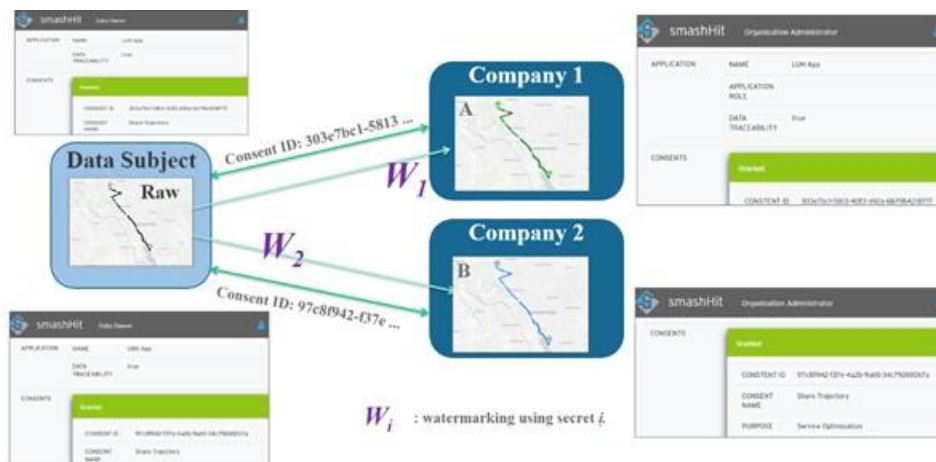
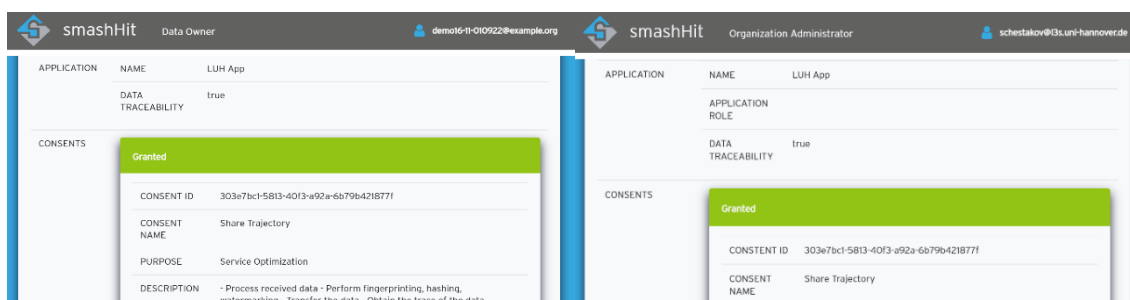


Figure 19: Consents granted and trajectories shared



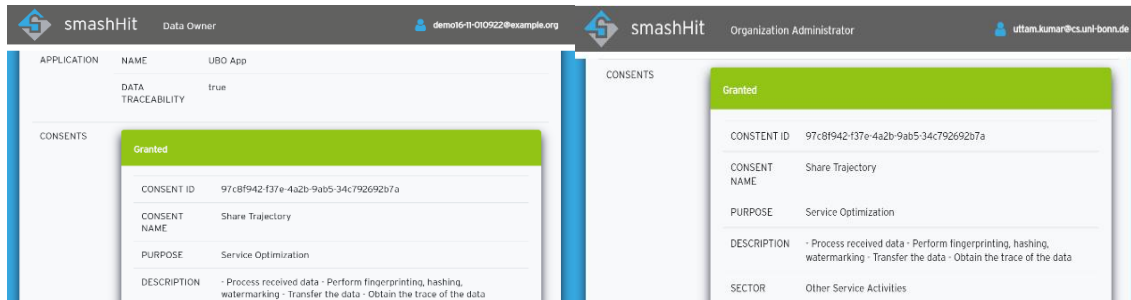


Figure 20: Consent granted for company 1 (LUH) on the top, company 2 (UBO) on the bottom

Figure 21 presents the discovery of the leaked data by the data subject (top left corner) since the data subject recognizes his path from work to home used by an unknown company, not present in any consent that was granted. Given this discovery, the data subject wants to understand which of the consent granted was leaked in case there was a leakage. On the bottom left corner, we can see how the data subject uses the data recognized from the third party (that we call leaked data) and checks the correlations against the data shared under each consent. The goal of the correlation computation is to understand if the secret/watermark present in the leaked data corresponds to the secrets/watermarks used during the watermarking process of the raw data to obtain a watermarked data for a given consent. The correlation is a score ranging from -1 to 1 , -1 meaning that it is very unlikely that the watermark in the leaked data matches the watermark of the data under the selected consent, and 1 meaning that both watermarks perfectly match. The results of the correlation computation in our scenario show a score of -0.34 against the data of company 1, whereas the score for the data of Company 2 is 0.95 . From this result, the data subjects understands that the leakage comes from the data shared with Company 2.

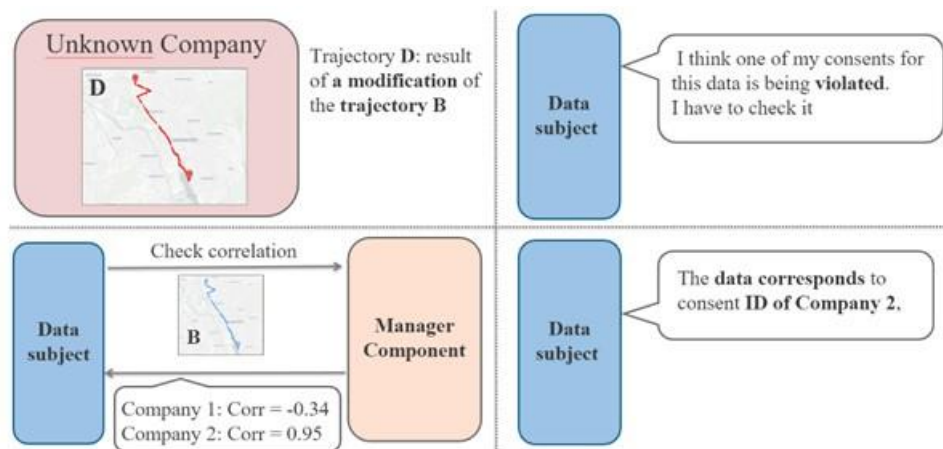


Figure 21: Leaked data discovery and leakage check

3 Glossary

ACT: Automatic Contracting Tool

B2B: Business-to-Business

B2C: Business-to-Consumer

B2G: Business-to-Government

Consent: As per Article 4(11) of the GDPR, 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

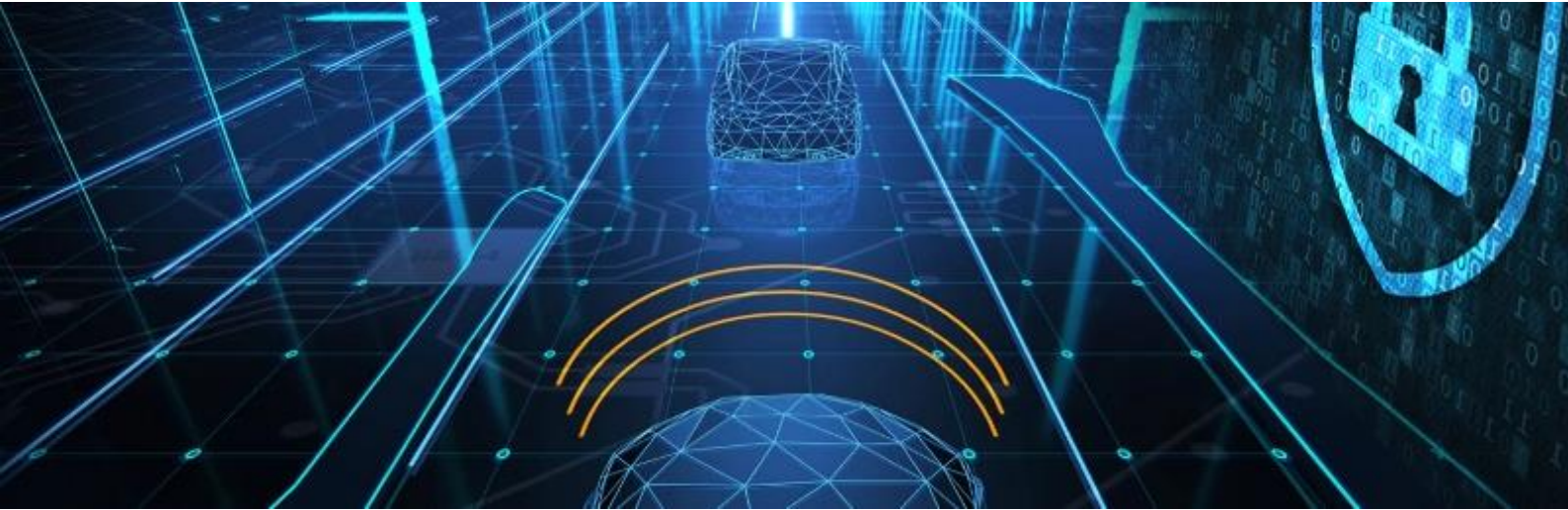
GDPR: Abbreviation for 'General Data Protection Regulation', a legal norm on EU level adopted in 2016, which is directly applicable within its scope and lays down rules for the processing of personal data so as to protect natural persons' fundamental rights and freedoms, in particular their right to the protection of personal data

OEM: Original Equipment Manufacturer

Personal data: Any information which are related to an identified or identifiable natural person (GDPR Art.4 (1))

RTD: Research and Technological Development

UI: (Contracting) User Interface



➤ **Our vision** - Solving Consumer Consent & Data Security for Connected Car and Smart City



➤ **Further information**

More information about smashHit, recent blog posts, the publications created within the project and other material like white papers and guidelines for users and developers can be found on our project website:

<https://smashhit.eu>

➤ **Our consortium**



Funded by the Horizon 2020
Framework Programme of the
European Union

Every effort has been made to ensure that all statements and information contained herein are accurate, however the smashHit Project Partners accept no liability for any error or omission in the same.

© 2022 Copyright in this document remains vested in the smashHit Project Partners.

