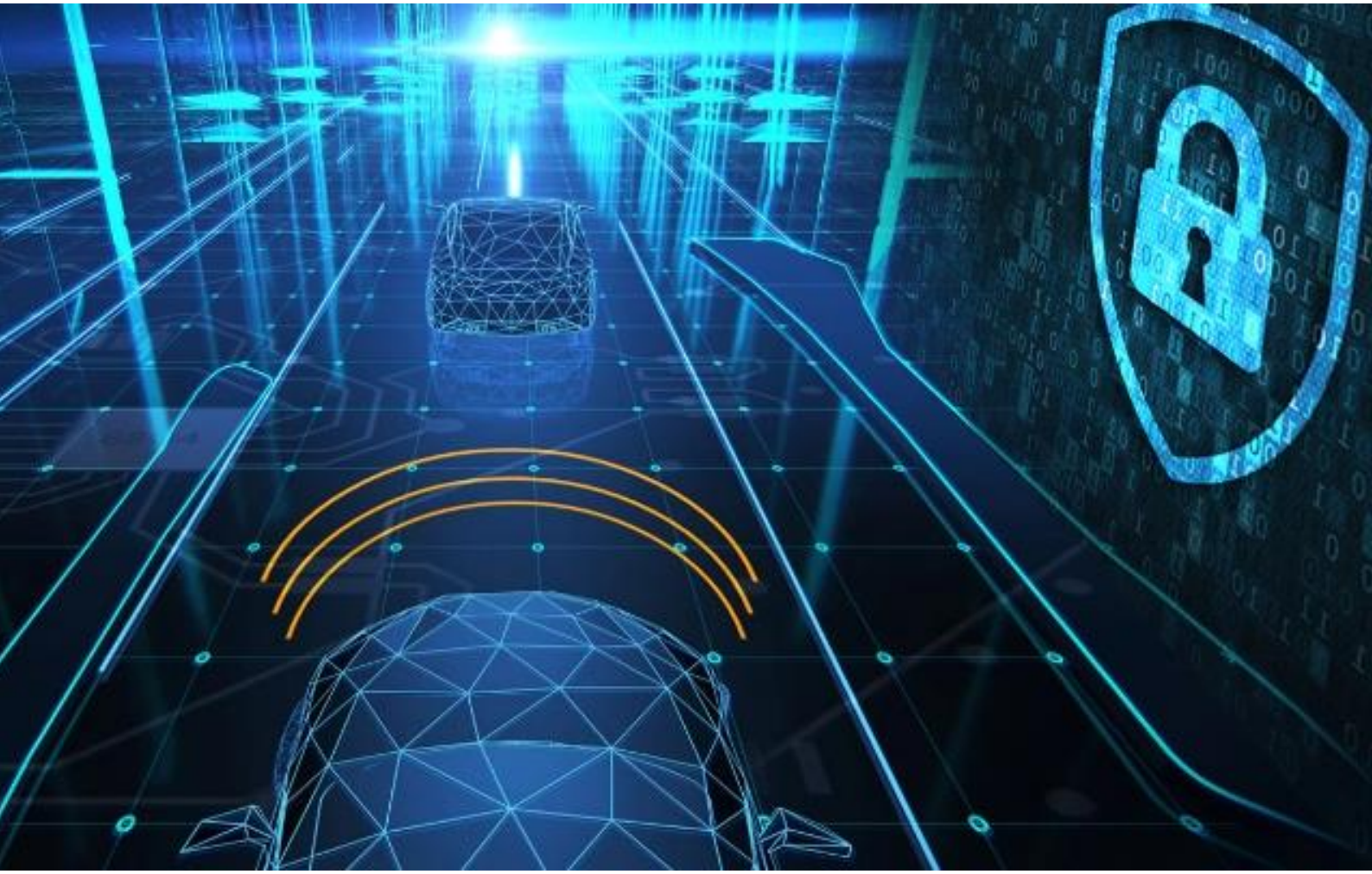
smashHit

Smart Dispatcher For Secure And Controlled Sharing Of Distributed Personal And Industrial Data

smashHit Concept

White Paper



October 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 concept white paper. 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[1], data providers[2] and data controllers[3]) to overcome existing barriers, as e.g. the complicated and time-consuming consent/contract processes, hindering to build-up 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, secure and integrating privacy-by-design reference Framework 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 win 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 presented (see smashHit project website).

In this report you will find some more details about the smashHit system concept as a whole, leading from today's constraints in consent/contract processes to how smashHit is facing those challenges with its innovative trusted and secure system concept.

If you got 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

[1] The person to whom the data relates to. The term is a legal attribute (Art. 4 Nr. 1 GDPR). The data subject can be the device owner at the same time. If the data relates to another person (e.g. the co-driver/another passenger) then the device owner is not the data subject. In this case the data subject will be e.g. the co-driver/the other passenger

[2] Data provider application and user: They get the consent to collect data from user devices according to the user consent

[3] A legal or natural person, an agency, a public authority, or any other body who, alone or when joined with others, determines the purposes of any personal data and the means of processing it

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.

The following key points will refer to those main innovative features and show the high future potential of the smashHit framework concept:

1 Challenges on the way to build a framework for assuring trusted and secure sharing of data streams

The vision of smashHit is to overcome obstacles in the rapidly growing Data Economy which is characterized by heterogeneous technical designs and proprietary implementations, which block business opportunities due to inconsistent consent and legal rules among different data sharing platforms actors and operators. The Framework provides methods and tools, such as the smash-Hit platform, to assure common consent over data shared by using semantic models of consent and legal rules. The new tools include consent management and automatic contracting among the data subjects, data providers, service providers and users. It also includes traceability of use of data.

These tools are critical for enormous volumes on data streaming from the usage of mass products with cyber physical features (e.g. vehicles). These data streams offer new opportunities to build innovative services, but their combination with other personal and industrial data is subject to complex ownership and consent aspects, data streaming from these products might be considered as personal data and there are many different and partially conflicting interests involved regarding the use of data generated by the use of such products. The project has been based on the solutions developed in previous projects (AutoMat, Cross-CPP, CAMPANEO, DALICC etc.). smashHit is driven by two industrial Business Cases involving several existing industrial and personal data platforms owned by the leading data providers in three diverse sectors (automotive industry, insurance, and smart city). Demonstrators of various applications of the developed solutions are being developed and will be shown latest from end of the project on.

The smashHit project vision as well as a range of selected key problems and needs in the state-of-the-art solution for consent and contract handling in the data economy led to the starting point of the smashHit project. Driven by these needs, innovative approaches were compiled to build the smashHit architecture as key element of the project.

1.1 Motivation

In the last years many data sharing platform approaches for different purposes (like B2B data exchange, data marketplaces or data processing services) emerged, giving cross-sectorial industries access to the great spectrum of sensor data coming from high volume products from various industrial sectors (vehicles, smart home devices, smart cities data etc.). With the increasing number of connected sensors and actuators within such mass products (so called cyber physical products), this number will rise exponentially in short-term. This enormous amount of data offered by various data sharing platforms represent:

- a massive information resource to create new value, allowing the improvement of existing services or the establishment of diverse new innovative services, by combining data streams from various sources
- a major big data-driven business potential, not only for the manufacturers of Consumer Products (CP), but in particular also for cross-sectorial industries and various organisations with interdisciplinary applications

The majority of these data sharing platform approaches offer a scalable, secure and trusted sharing of data. However, they all lack in the provision of solutions for consent creation, management and observation between two or more involved actors that aim to share personal data. To fully exploit data sharing approaches in practice, they have to consider national and international laws like the European General Data Protection Regulation (GDPR). Among others, such regulations define that data subjects can decide by whom and for which purposes their data can be used;

they define how data providers have to handle data and they define how data have to be processed. A data sharing platform that considers such regulations needs an additional layer of consent creation linked to a contract which would guarantee the compliance with all requirements of the contracting parties and national and international laws. This gap needs to be filled and is where smashHit aims to bring an added value.

1.2 Challenges & Steps towards the smashHit Framework Solution

As mentioned above, the rapid growth of the Data Economy is also reflected on the number of B2B, B2C and B2G data-sharing platforms recently launched, which are contributing to fragment the market, preventing business opportunities due to lack of interoperability, inconsistent consent and legal rules among different data-sharing platforms actors and operators.

There is a short-term challenge for the data economy to look for an interoperable data-sharing platform to enforce and manage multi-platform agreements for exchanging data whilst protecting and assuring compliance with GDPR, Privacy and Security Policy enforcement rules of individual data providers, national (country) data privacy and protection rules and EU-legal directives and legislation surrounding personal and industrial data generation, storage and sharing. Due to this high level of market fragmentation, the situation today is characterized by far too complex and individual value chains resulting in economic inefficiency. Therefore, the use and integration of data from various platforms is limited due to missing solutions for agreement on consent, legal rules, effective contracting, data use traceability, security & privacy issues etc.

The requirement analysis at the beginning of the project has shown that this situation is mainly characterised by the following major challenges and barriers for all stakeholders in the value chain, the service providers (data processors) and for the CP manufacturers (data providers) and the CP owners (data subjects):

- The number of steps required to gain consent create customer “friction”.
- Time taken to obtain the required consent is too long.
- Verifying a person giving consent is often insufficient as well as duplicated at each consent step.
- Problem of broken consent chain is unsolved.
- Lack of tools to prevent data misuse prevent willingness of data providers to provide data.
- Insufficient control for data subjects over their data.
- Missing support in creating legally binding contracts.

In contrast to today's fragmented data sharing landscape, which is characterised by non-heterogeneous technical designs and proprietary implementations and by this means is hindering the use and integration of data from various platforms due to missing solutions for effective consent/contracting and data use traceability etc., the smashHit project focuses on user-oriented solutions that make data marketplaces more attractive and trustful for its key stakeholders. Therefore, smashHit has to overcome several obstacles by establishing an inter-data-platform solution enabling simplified multi-platform consent/contract processes for exchanging data also ensuring a trustful data use traceability. To achieve these key challenges, smashHit needed to develop the following main characteristics:

- **Improve citizens trust** by means of tracing the use of data over diverse platforms
- **Improve OEM & data customer's trust** by means of fingerprinted data to ensure traceability/unchangeability along value chain and data quality, as well as consent tracing -> notification of all involved contractors in case of broken consent chain
- **Simplify consent process** through authentication of the individual (certification of consent) and single point of consent (management and distribution of consent)
- **Support in consent/contract generation** by supporting the digital creation of contract texts, and taking relevant legislations/legal rules into account

Such an innovative inter-data-platform platform solution will have several positive effects on the European Data Economy, as e.g.:

- To overcome existing barriers, as e.g. the complicated and time-consuming consent/contract processes
- Increase trust for all stakeholders in the data market, due to a strong data traceability mechanism
- Increase willingness of data providers (OEM) to provide CP data for 3rd party use
- Open new opportunities for value-creation by creation of innovative services using data from multiple platforms

Data subjects need a solution that would enable them to easily trace the use of their data over diverse platforms. The solution must provide the data subject the power to manage their data, enabling them to identify for each of their products, who gets which product data, for which purposes they are used and how long is the contract run-time. In addition, the solution has to simplify consent processes, to create the trust and motivate the users to share their data by offering solutions users find useful and necessary.

Data providers (e.g. OEMs) need a solution that allows to identify the origin of a data leakage in case of data misuse in an efficient way. Further they need to have the possibility to monitor if given consent is broken. Both cases have a high risk of reputation damage for the data provider.

Generally, we can state, that a reliable solution to eliminate the above data traceability challenges related with the 'reconstruction of data leakage' and minimisation of 'reputation damage risks' will considerably increase the willingness of large CP manufacturers to provide more data from their products.

Data controllers as the processors of the data subject's data are offering services based on data from various data platforms. A key request for them is to simplify the process to obtain consent and easy contracting. Moreover, data controllers have similar needs w.r.t. data traceability as described for data providers, e.g. regarding identification of broken consent chain or backtracking of data misuse.

Service customers have similar need as the data subjects, and may even be considered as data subjects for most situations, as e.g. simplified consent/contract processes and a clear traceability of data usage for all their products.

Finally, **Legislators** need a solution which enables to apply their laws in a technical way. A unified solution would also simplify the controlling of law compliance in the data economy.

2 The smashHit Framework Solution to meet the challenges

smashHit started with the aim to design and implement a trusted, secure- and privacy-by-design reference platform to simplify the consent/contract process as well as to enable consent tracing and sharing among multiple data platforms, as well as offering solutions to identify data misuse as well as to support data customers in creating contract documents. The solution addresses the identified needs of different actors in the data economy. Therefore, smashHit provides answers for these needs compiled in the shape of a smashHit Platform which can be divided into five different main building blocks shown in the following figure, which build the **key innovations** of the project. These building blocks are partly using basic concepts of state-of-the-art technologies that can be used for further exploitation to fill the identified gaps.

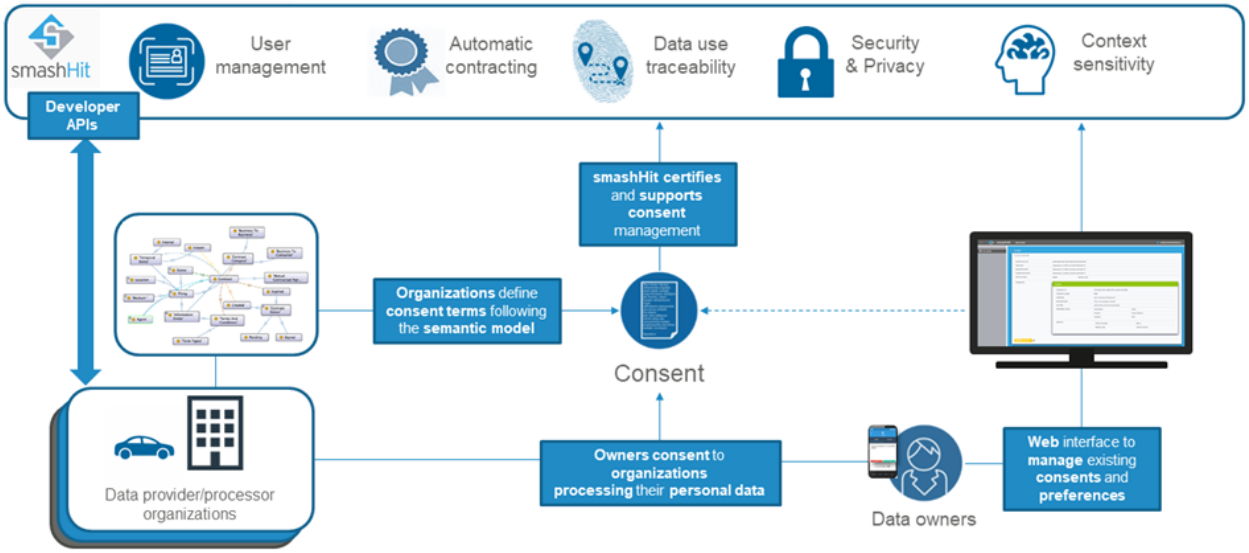


Figure 1: smashHit framework solution conceptual module overview

2.1 smashHit Platform

The smashHit platform module provides the basic functionalities within the overall smashHit framework solution. Different actors aim to get consent creation, management and observation functionalities. In particular it covers the following:

- **User management functions** – This component includes the functionality regarding the life cycle of the actors involved in the smashHit framework. It interacts with the user database which stores information related to user accounts.
- **Semantic model of consent and legal rights** – This component represents the used core ontology and resulting semantic data model for the description of legal rights, consents, context and automatic contracting rules, terms and conditions.
- **Context sensitivity solution** – This component adds context sensitive features to the overall smashHit framework and enables a context dependent behaviour of the system, e.g. monitoring of user preferences.

Figure 2: Consent Certification process

As part of the smashHit platform, the **Consent Certification Module** includes functionalities along the life cycle of consent certificates and is a core component of smashHit. The module includes functionalities for consent management and support. Semantic models are used to describe consent (-chains) between two or more participants. The described consent will be digitally certified and saved in a database. This approach will enable to manage and control consent about data usage with two or more involved participants in the Data Use Traceability module. Figure 2 shows a simplified look at a consent certification process. The actual process is not linear and some steps were simplified (such as the registration process) to make for an easier reading of this paper however is presents a good overview.

2.2 Automatic Contracting

The smashHit solution accelerates the consent creation process to increase the efficiency in the data economy and to reduce the efforts needed for a consent creation and consent management. This component aims to allow a semi-automatic consent form creation process based on compliant data usage and processing rules. This approach is based on ontologies and reasoning technologies (having the smashHit semantic model as basis). Construction and management of contracts based on specific terms and conditions in compliance with GDPR is another service provided by the ACT. It provides a flexible yet meaningful model for data sharing in smart city and insurance domains under different circumstances.

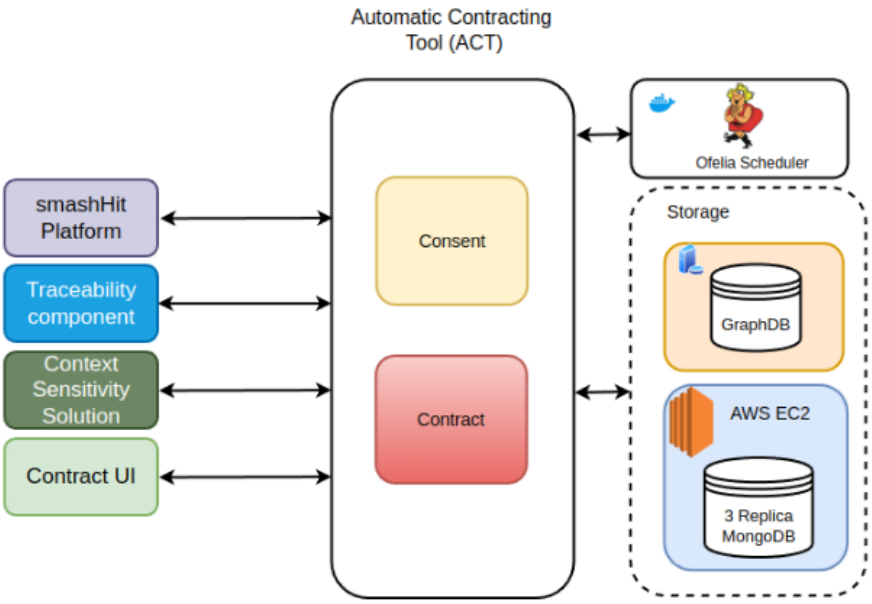


Figure 3: Automatic Contracting Tool component architecture

Data subjects need a solution which provides monitoring functionalities over their data. This is enabled by the consent certification in the previously described module. Certified contracts and consent(-chains), saved in a knowledge graph enables to always have an overview about signed contracts and consents, and enables the tracing of consent, allowing the identification of a broken consent chain.

2.3 Data Use Traceability

The data use traceability component has two purposes: (1st) to trace data flows by applying hashing, fingerprinting/watermarking, and (2nd) the identification of data leakages using the same tools. Those tools are used to make the data recognisable even after some modifications. The component addresses the need of OEMs, data providers and data controllers to get a solution which enables the identification of data leakages or misuses. Basis for this component are data hashing, fingerprinting and watermarking technologies that shall enable the identification of the last data source within the smashHit ecosystem. The data hashing combined with fingerprint or with watermarking provides answers about where the leaked or misused data was located or forwarded the last time which will avoid the blaming of guiltless participants in a consent chain. Figure 4 shows from 1) to 6) an example of how the information flows within all stakeholders of the smashHit ecosystem.

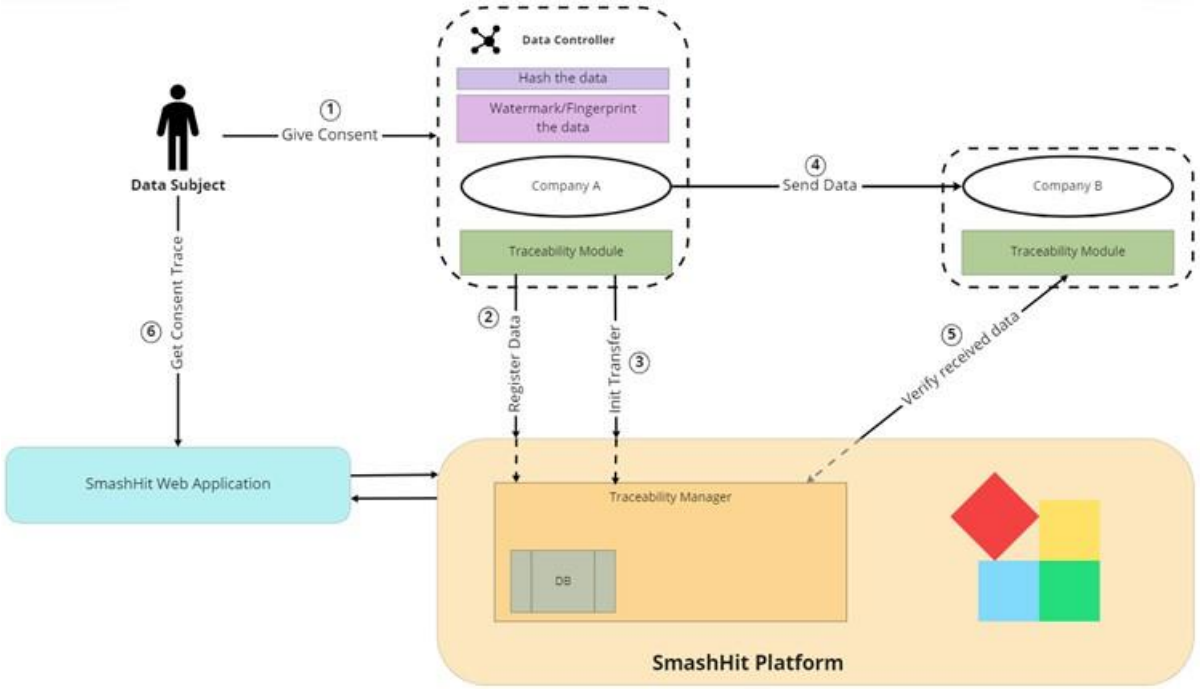


Figure 4: Data Use Traceability component: example of information flow within all stakeholders of the smashHit ecosystem

2.4 Security and Privacy Mechanisms/Metrics

The smashHit Platform is developed and runs in accordance with the General Data Protection Regulation (GDPR). The principles of privacy by design and by default have been cornerstones for the development of the smashHit infrastructure. The security & privacy policy languages and mechanisms support compliance with security and privacy policies represented and applied within the smashHit platform and connected data processors.

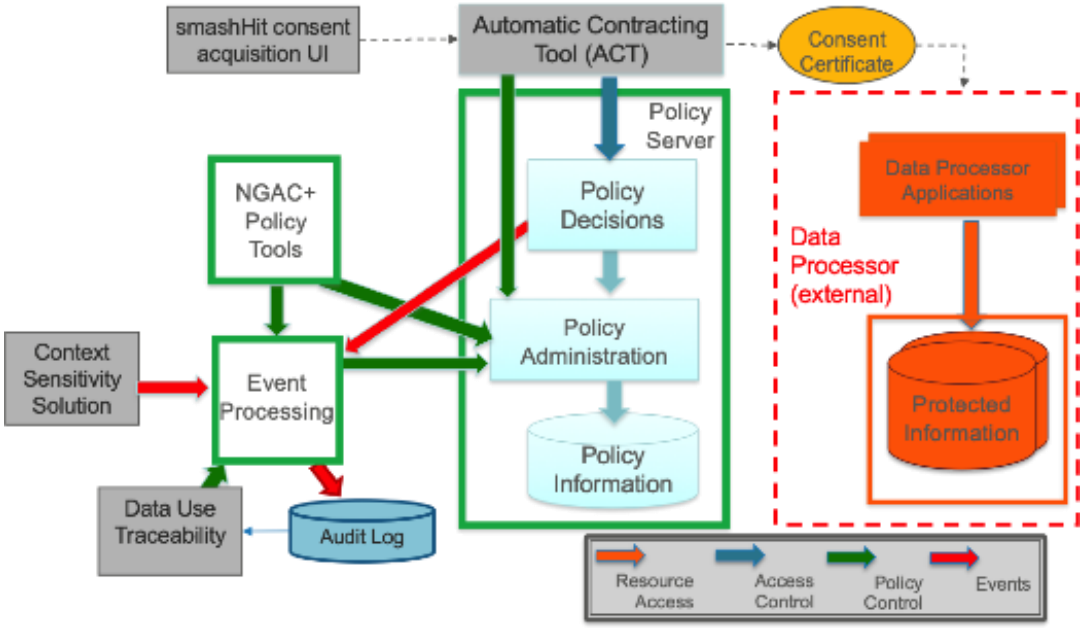


Figure 5: Security and Privacy component architecture

The Security and Privacy mechanisms combine privacy/security policies of data subjects and data controllers/processors in a complementary way. The Policy Server makes policy decisions based

on policy information and context, including consent information gathered through the consent acquisition UI and provided by the ACT through policy administration. As granted by policy decisions, the ACT issues a Consent Certificate that external data processors apply to control access to protected personal information. Events reported to the Security and Privacy Event Processing may provide information to smashHit Data Use Traceability (see Figure 5). Security Metrics assess the smashHit Framework's quality of conformance to governing regulations and other norms.

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

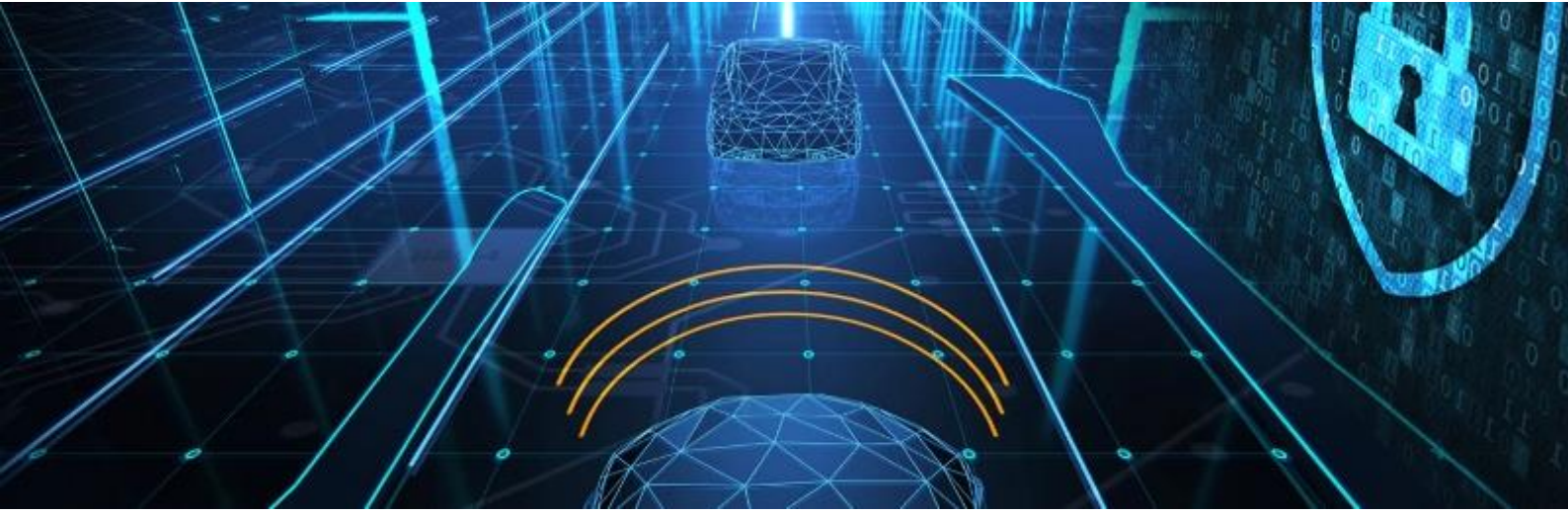
GDPR: Abbreviation for 'General Data Protection Regulation', a legal norm on EU level adopted in 2016, which is directly applicable within its scope and lays down rules for the processing of personal data so as to protect natural persons' fundamental rights and freedoms, in particular their right to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



smashHit

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

Further information

This document is part of the smashHit Methodology. The complete set of documents, including user/developer guides as well as other white papers created within this scope can be found on our website:

https://smashhit.eu/publications

Our consortium

ATB

universität innsbruck
Department of Computer Science

Leibniz Universität Hannover

LexisNexis RISK SOLUTIONS

THE Open GROUP

infoTripla

UNIVERSITÄT BONN

Atos

FORUM VIRIUM HELSINKI

Funded by the Horizon 2020 Framework Programme of the European Union