5G HarmoniseD Research and TrIals for serVice Evolution between EU and China

T5.4 Security and privacy aspects of 5G and the Internet of Vehicles in Future 5G Vehicular Networks

WHITE PAPER

Adrian Quesada Rodriguez (MI); Renáta Radócz (MI); Cédric Crettaz (MI); Abdelwahab Boualouache (Uni.lu); Ridha Soua (Uni.lu); Sébastien Ziegler (MI), Kinga Képessy (MI), Anna Kourakli (MI)

This white paper summarizes the different actions undertaken by 5G-DRIVE towards identifying solutions that could enable secure and privacy-friendly data communications in 5G future vehicular networks. The contents of this white paper reflect the main outcomes of T5.4 of the 5G-DRIVE project, as described in further detail in Deliverable 5.3. The methodology followed by this deliverable aims to meet two main objectives: 1) the identification of relevant personal data protection and security requirements in dissimilar legal frameworks (EU-China) and standards (ISO, ETSI, ITU, ECCP, etc.); and 2) the identification of innovative methods to address these requirements; and future 5G Vehicular Networks, centering on security and personal data protection.

To this end, an analysis of the relevant legal frameworks was carried out and followed by an identification of relevant standards and the identification of the key personal data protection and security requirements. This action was focused on the identification of viable, interoperable, and strong network-level oriented technical and organizational requirements in two main areas: regulatory compliance (with a focus on the organizational actions that will be necessary for an eventual deployment of a future 5G Vehicular Network); and V2X security and personal data protection (In close alignment with 5G-DRIVE WP4). Afterwards, a set of technical and organizational solutions were examined as potentially viable for the development of secure and personal data protection enabled 5G Vehicular Networks.

A) Legal Assessment

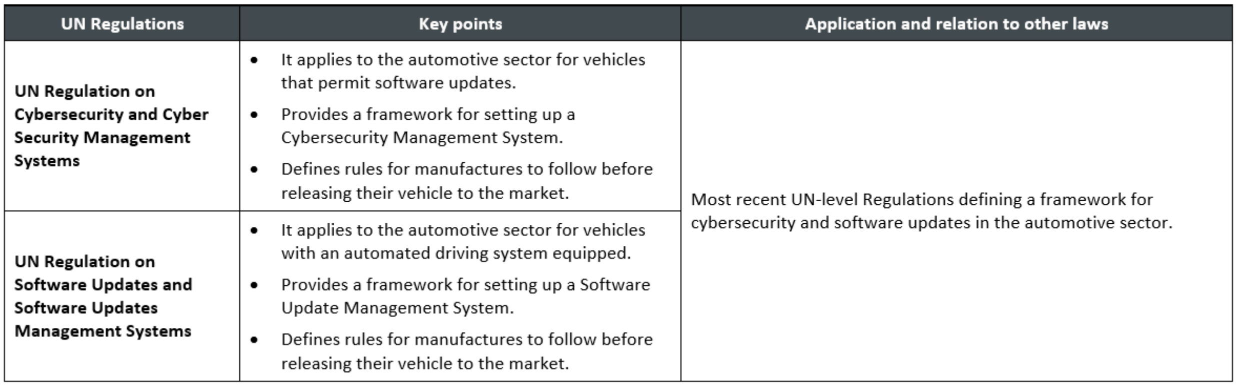
As previously noted, the task carried out a comprehensive assessment of the legal and standardization frameworks surrounding 5G, V2X and future vehicular networks to identify the key issues surrounding the topic, identify key requirements for personal data protection and finally enable the proposal of relevant technical and organizational solutions. In recognition of the partners and goals of the 5G-DRIVE project, special emphasis was given to the identification of commonalities and differentiators between the European and Chinese legal frameworks. The following table summarizes the key outcomes of this process:

• Uses the definition of personal data and data subjects • Prior notice and consent (different legal bases for the processing of personal data) • Emphasis on data controllers and data processors • Data breach notification requirement to the supervisory authority and/or data subject • Independent Supervisory Authorities • Limiting further processing • Strong data minimization requirement • Specific requirements for sensitive data (e.g. biometric data, religious beliefs, genetic data, ethnicity, etc.) • Right to be forgotten is strongly enforced • Right to data portability • Personal data protection given human right level • High level of requirements for international data transfers • Voluntary certification system	• Used the definition personal information and personal information subjects • Prior notice and consent (lighter rules and does not require implicit consent) • Emphasis on network operators' obligations • Data breach notification requirement to authorities and data subjects but does not specify the timeframe or information • There are no specific supervisory authorities set up, however, the Cyberspace Administration of China handles enforcement efforts regionally • Limiting further processing • Softer data minimization requirement • Specific requirements for sensitive data but different definition (broader, risk-based definition) • Right to be forgotten is limited to specific cases • Right to data portability • No privacy-related restrictions for the generation of solutions • Conceptualized as national security • Voluntary certification system

A.1) Relevant International Regulations

Legal and regulatory work for the realization of sustainable mobility and the introduction of autonomous vehicles is centralized at United Nations Economic Commission for Europe (UNECE). It hosts multilateral agreements and conventions ruling the requirements related to the use of these new technologies (e.g., safety measures, connectivity, cybersecurity, testing methods, and safe integration) while liaising with relevant stakeholders. The UNECE also hosts the intergovernmental platform of the World Forum for Harmonization of Vehicle Regulations that defines technical requirements in the automotive sector. The World Forum created a dedicated Working Party on Connected Vehicles (GRVA) in 2018, where countries from all over the globe participate to mobilize their expertise.

The UNECE started its work in 2014 and successfully amended the 1968 Vienna Convention on Road traffic to allow autonomous vehicles in traffic and removed the 10 km/h limitation for autonomous systems included in the UN Regulation No. 79. In June 2020, the UNECE published its proposal for two new UN Regulations on cybersecurity and software updates after recognizing the threatening nature of cyberattacks against vehicles. Both Regulations came into force in January 2021. The following table summarizes their main characteristics:



UN Regulations	Key points	Application and relation to other laws
UN Regulation on Cybersecurity and Cyber Security Management Systems	- It applies to the automotive sector for vehicles that permit software updates. - Provides a framework for setting up a Cybersecurity Management System. - Defines rules for manufactures to follow before releasing their vehicle to the market.	Most recent UN-level Regulations defining a framework for cybersecurity and software updates in the automotive sector.
UN Regulation on Software Updates and Software Updates Management Systems	- It applies to the automotive sector for vehicles with an automated driving system equipped. - Provides a framework for setting up a Software Update Management System. - Defines rules for manufactures to follow before releasing their vehicle to the market.	

A.2) European Legal Framework

In Europe, the General Data Protection Regulation (GDPR) has generated an interesting landscape for the integration of these two technologies in connected or smart vehicles. The European legal framework has included specific personal data protection requirements which extend to the use of innovative technologies such as V2X and 5G, and regulatory authorities and oversight bodies have expressly generated both legal requirements, guidelines, and best practices to address the potential risks these technologies generate vis-à-vis data subject rights.

In this context, the assessment began by considering the General Data Protection Regulation (GDPR), which, amongst other elements, includes requirements for consent and the rights of data subjects, obligations of data controllers, Data Protection by Design and by Default approach, Data Protection Impact Assessments (DPIAs) and creates a voluntary certification system to demonstrate compliance with data protection.

Following this, the project examined the Directive on Privacy and Electronic Communication (ePrivacy Directive) and the European Union Regulation on Privacy of Electronic Communication (ePrivacy Regulation) is the reference legal framework for electronic communications. They provide for requirements for security and confidentiality of communication, protection of traffic and location data and lastly, protection of the end-user terminal equipment and fundamental rights and freedoms, such as the respect for private life in the electronic communications sector. The Directive on Security of Network and Information Systems (NIS and NIS 2) is another important legislation on cybersecurity, providing for measures to guarantee the security of the European Union's cyberspace through a cybersecurity strategy.

Another important normative framework for providing secure and seamless electronic interactions between users of 5G vehicles, 5G service providers and public authorities is the Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation). Lastly, it is worth mentioning that the EU Directive 2018/1972, establishing the European Electronic Communications Code, lays down rules for regulating the electronic communications networks, telecommunications services and related facilities and services, while the EU Cybersecurity Act introduces a European cybersecurity certification system, which ensures that certified products, processes, and services meet specific cybersecurity criteria.

The following table summarizes the main takeaways from the analysis of the European Framework:

The General Data Protection Regulation (GDPR)	It sets: • rules for free movement of data. • requirements for consent and the rights of data subjects. • obligations of data controllers, Data Protection by Design and by Default approach, DPIA etc. • a voluntary data protection certification (art. 42). system to demonstrate compliance	The main European Union regulatory framework in the field of personal data protection. Intrinsically related to the ePrivacy Regulation.
The Directive on Privacy and Electronic Communication (ePrivacy Directive) and the European Union Regulation on Privacy of Electronic Communication (ePrivacy Regulation)	It provides for: • requirements for security and confidentiality of communication, protection of traffic and location data and protection of the end-user terminal equipment. • fundamental rights and freedoms, as the respect for private life in the electronic communications sector.	With respect to the GDPR, the ePrivacy Regulation will be considered *lex specialis*. Addresses further aspects of electronic communications networks that may affect the rights and freedoms of data subjects. It does not include any specific provisions for data retention.
Directive on Security of Network and Information Systems (NIS Directive)	• It is a legislation on cybersecurity, measures to guarantee the security of the European Union's cyberspace.	Digital service providers are covered by the NIS Directive regime upon the sole transposition of the directive into Member States' national law. Essential services are only covered by the scope of the NIS Directive upon designation as such by the respective Member State.
Revised Directive on Security of Network and Information Systems (NIS 2 Directive)	• It strengthens Europe's collective resilience to cyber threats. • It ensures that all citizens and businesses can take full advantage of reliable services and reliable digital tools. • It aims to address existing and future cyber and non-cyber threats.	The revised NIS presents a new EU cybersecurity strategy for shaping Europe's digital future. The EU Cybersecurity Act has equipped Europe with a framework for cybersecurity certification of products, services and processes and strengthened the mandate of the EU Agency for Cybersecurity (ENISA).
Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation)	• It provides for mutual recognition and interoperation of cross-border eID management, trust services and certificates. • Its primary objective is the 'unique identification' of a person. • It defines predetermined Level of Assurance. • It clarifies that unanimous persons' identification takes place by transmitting a minimum dataset which should include a Persistent Unique Identifier. • It sets requirements for considering electronic identification systems compliant.	Since the GDPR repealed Directive 95/46/EC, all provisions of the eIDAS Regulation have to be interpreted and applied in accordance with the GDPR.
Directive (EU) 2018/1972 of the European Parliament and of the Council establishing the European Electronic Communications Code	• It rules for the regulation of electronic communications networks, telecommunications services and related facilities and services.	It is without prejudice to measures taken at the Union or national level, in accordance with Union law, relating to the protection of personal data and privacy. In respect of the information exchanged, Union data protection rules shall apply (Article 11). Encryption should be mandatory in accordance with the principles of security and privacy by default and by design.
Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (Cybersecurity Act)	• It introduces a European cybersecurity certification system. • The system ensures that certified products, processes and services meet specific cybersecurity criteria.	The first EU Regulation to meet the security challenges of connected products, Internet of Things (IoT) devices and critical infrastructure through such certificates.

A.3) Chinese Legal Framework

On the other hand, the Chinese approach has relied mostly on the specification of legal requirements and the generation of standards to be addressed through voluntary certifications by relevant industry players. The People's Republic of China Cybersecurity law and the Cyberspace Administration of China Measures on Cybersecurity Review establish baseline obligations for networks operators which seek to ensure the defense of critical infrastructures, clarify data localization requirements, ensure security inspections, and protect personal information. These elements are complemented by the Cyberspace Administration of China Draft Measures for Data Security Management and the Draft Measures on Security Assessment of the Cross-border Transfer of Personal Information, which provide detailed guidelines on how the security assessments should be operated. These legal dispositions are then also complemented by the Law of the PRC on the Protection of the Rights and Interests of Consumers (Consumer Protection Law).

Two draft laws were also examined throughout this process, namely the Draft of the Personal Information Protection Law (PIPL Draft) and the Data Security Law of the People's Republic of China (Draft).

The following table summarizes the main takeaways from the analysis of the Chinese legal framework:

The People's Republic of China Cybersecurity law (Cybersecurity Law)	• Cybersecurity and protection of privacy. • Internet surveillance for national security purposes. • Obligations of networks operators, defense of critical infrastructures, data localization requirements, security inspection and protection of personal information.	These provisions have been implemented by the Cyberspace Administration of China.
Cyberspace Administration of China Measures on Cybersecurity Review	• Contains the obligations of operators of critical information infrastructure. • Defines the scope of network products and services that include the core network equipment, high-capability computers and servers, high-capacity data storage, large databases and applications, network security equipment, as well as cloud computing services. • Sets up a review body with the lead of the CAC.	Following Article 35 of the Cybersecurity Law, operators of critical information infrastructure must undergo a security review China's national security is impacted by the procurement of networks products and services; the Measures on Cybersecurity Review intends to further define the means of doing so.
Cyberspace Administration of China Draft Measures for Data Security Management	• Provisions in relation to data collection, retention and consent. • Defines important data and sets specific obligations in relation to its collection.	The Draft Measures provide detailed guidelines on how the security assessments should be operated and is intended to complement the Cybersecurity Law of China.
Cyberspace Administration of China Draft Measures on Security Assessment of the Cross-border Transfer of Personal Information	• Procedure to export personal information outside China's cyber-jurisdiction. • The contract between the network operator exporting personal information and the foreign data recipient can be compared to a data transfer agreement or to the binding corporate rules of the GDPR.	
Law of the PRC on the Protection of the Rights and Interests of Consumers (Consumer Protection Law)	• Consumers have the right to safety, choice, truthful information, fair treatment, to form social organizations and fair compensation. • Protects consumers' personal information and sets rules for business operators. • Requires providing explicitly the purpose, method, scope for collecting or using information and ensuring consumers' consent.	The Advertising Law is another legislation that is related to the Consumer Protection Law. The definitions of advertisement and advertisement publishers are very broad and cover almost any sort of product or service promotion.
Draft of the Personal Information Protection Law (PIPL Draft)	• China's first comprehensive law on personal data protection. • Transparency, accountability, fairness, purpose limitation, data minimization, data retention and accuracy, principles provided by the draft PIPL (similar to GDPR principles). • Management and security measures (through compliance audits, risk assessments, data breach reporting and more) as in GDPR.	It is broader than GDPR, as personal information also refers to financial account information and the location of the individual. Narrower than GDPR, as it leaves out of the scope of the definition of personal information the trade union membership, political opinions, genetic and biometric data and information related to sexual life. In contrast to PRC Cyber Security Law, it puts forward an overseas extraterritorial application to individuals and entities. Unlike the GDPR, there are no provisions for adequacy determinations in third countries. In contrast to GDPR, it requires security assessments in case of abroad personal data transfer. More expansive data localization requirements and clearer rules on cross-border transfer of personal data.
Data Security Law of the People's Republic of China (Draft)	• Required steps to ensure data security is reached.	New power and responsibilities for government bodies and private actors, together with the Personal Information Protection Law.
Chinese Standard: Information Security Technology – Personal Information Security Specification GB/T 35273-2017 (CPISS)	• A voluntary framework detailing the best practices for compliance with China's data protection laws.	It creates a voluntary system that is aligned with the GDPR. It adopts general principles that can be found in most data protection laws. Establishes several rights to match the rights conferred to data subjects by the GDPR and includes a purpose limitation requirement. In accordance with the Cybersecurity Law, prior notice and consent from personal information subjects is necessary when non-de-identified personal data must be shared or transferred. Key reference when considering potential applicability of certification solutions for international data transfers.

A.4) Relevant International Standards

Having compared the European perspective with the Chinese perspective, the task performed a review of the relevant international standards and recommendations on connected vehicles management, such as as the IEEE 1609 Wireless Access in Vehicular Environment (WAVE) Working Group Standards Family, the ITU-T SG 17 Recommendations, the ISO/IEC 27000:2018 – Information Security Management System (ISMS) family of standards and lastly, as well some other ISO and ETSI standards.

The following table summarizes the main takeaways from this assessment.

IEEE 1609 Family of standards	• Guidance on secure transmission of messages in Wireless Access in Vehicular Environments. • Standardize not only the architecture but the set of services and interfaces enabling wireless communications in vehicular environments. • Includes: IEEE 1609.0-2019, IEEE 1609.2-2016, IEEE P1609.2.1, IEEE 1609.3-2020, IEEE 1509.4-2016, IEEE 1609.11-2010, IEEE 1609.12-2019
ITU-T SG 17 Recommendations	• Promotion and production of standardization recommendations on communication technology. • Identifies security threats to connected vehicles and include security guidelines on effective prevention of attacks • Includes: X.1371, X.1372, X.1373, X.1374, X.1375, X.1376
ISO/IEC 27000 (ISMS) family of standards	• Establishes an information security management system within an organization. • Provides a framework for organizations to manage the security of their assets, information, or intellectual property. • Requires monitoring the risks to information security in an organization and examining possible threats and vulnerabilities. • Includes: ISO/IEC 27000:2018, ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC 27005:2018, ISO/IEC 27701:2019
ISO/IEC 29190:2015	• Different steps necessary to access the capability of an organization in the context of privacy.
ISO/TR 12859:2009 Intelligent Transport System	• Development of the architecture and design of all ITS standards, systems and their implementation. • A roadmap to developers of ITS devices on general data privacy and protection aspects.
ISO 24100:2010	• Promotion of safe deployment and expansion of probe vehicle information services.
ISO 16461:2018	• It is a further specification of ISO 24100. • Integrity of personal data and privacy of information gathered by probe vehicle systems. • Possible solutions for the protection of anonymity and integrity of probe data.
ISO/TR 17427-7:2015	• Awareness on possible privacy issues arising from the development, deployment and implementation of Cooperative Intelligent Transport System (C-ITS). • No specifications for solutions of these issues.
ETSI TS 102 940 v1.3.1 (2018-04)	• Identification of the functional entities necessary to support security in an ITS environment using a holistic approach. • Purpose and location of several security services in relation to the protection of transferred information and the management of the parameters necessary to security.
ETSI TS 102 941 v1.3.1 (2019-02)	• Trust establishment and privacy management to support security in an ITS environment.

B) Requirement identification

The work performed throughout this analysis enabled the identification of the challenges derived from the diverse range of legal requirements that become relevant in this context, which in turn served to guide the development of technical and organizational solutions. This was enabled through the identification of viable, interoperable and strong network-level oriented technical and organizational requirements in two main areas: regulatory compliance (with a focus on the organizational actions that will be necessary for an eventual deployment of a future 5G Vehicular Network); V2X Security (In close alignment with 5G-DRIVE WP4).

As for the first area, several requirements were identified as relevant for Connected Vehicle Personal Data Protection compliance, namely:

1) Enabling privacy safeguards by default
2) Identification of data categories
3) Protection of traffic data
4) Protection of location data
5) Data management / Data subject right compliance
6) Data retention compliance
7) Anonymization and pseudonymization
8) Keeping records of processing activities and disclosures
9) Data breach information
10) Encryption of personal data by default
11) Update and review of privacy measures
12) Security of processing (prevention of unauthorized access, alteration, disclosure, and destruction of personal data)

In addition to these elements, the following key requirements were identified as necessary to ensure V2X Security:

1) Identification, Authenticity, and Integrity (IAI)
2) Availability (A)
3) Confidentiality and Privacy (C&P)
4) Non-Repudiation and Accountability (NR&A)

C) High-level assessment of 5G-DRIVE Data Protection Compliance

Based on the identified requirements, a high-level assessment of the actions undertaken in the 5G-DRIVE project was then introduced, focusing particularly on compliance with personal data protection requirements. This assessment examined both eMBB and V2X trials with the main goal of showcasing the overall project compliance with data minimization and privacy by design requirements. The goal of this exercise was to identify any potential issues of relevance for the project, which should be considered by any of the project partners in case the eventual exploitation of the project results is sought after. Furthermore, it served to inform the technical and organizational solutions proposed subsequently. Given the highly contextual nature of this assessment, a summary will not be provided in this document, however it is available as part of 5G-Drive Deliverable 5.3.

D) Proposed Technical Solutions:

After a detailed overview of the most relevant legislative and standardization frameworks which have been considered throughout the research performed in 5G-DRIVE and which have inspired the range of possible solutions examined to tackle security and personal data protection risks, it is important to examine the potential and innovation capacity of 5G vehicular networks towards a safer, cleaner, and more efficient digital transformation. This is vital, as there are still numerous issues surrounding 5G connected vehicles: from (cyber)attacks that threaten not only the driver's (and their passengers') safety but others on the road; to additional concerns related to the privacy and security of the drivers as data subjects. Valuable work has been done by institutions and global organizations on the identification of issues and potential solutions related to vehicular networks for identifying potential technical and organizational solutions going beyond the state-of-the-art research to further address the intrinsic difficulties related to connectivity.

Network slicing is defined in the context of 5G as a key feature allowing a clear separation of the resources into virtual networks and comes with its own privacy and security issues. A slice is a virtual network having specific characteristics complying with requirements given for a specific use case. The usage of 5G network slicing implies the installation and the deployment of new components inside the 5G infrastructure. As consequences, new risks concerning data protection appear. As the 5G telecommunication network is built with all the components connected to each other on an IP architecture, the components are exposing their interfaces on the IP layer, including the Web- interfaces. So, the attack surface is becoming bigger and the possibilities to hack one or several components are naturally increased. In a classical server/client approach, there are two parties: the service provider running the server offering the service and the client consuming the service; in this case, data processing is performed server-side with the legal responsibility of the service provider, accordingly to the law where the service provider is located. Network slicing may then introduce new players (the network slicing service provider) which may act as data processors, carrying out data processing activities at the network slice infrastructure level. This introduces further complexity to the issues surrounding jurisdiction definition.

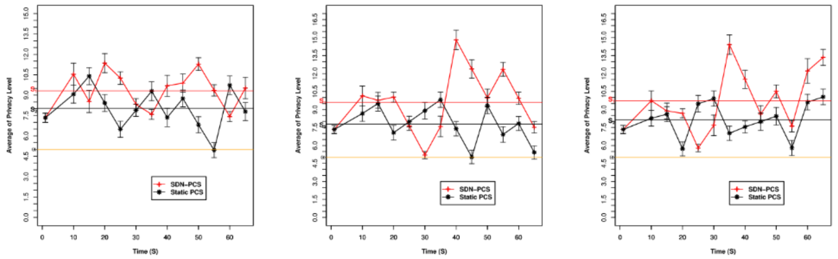
Furthermore, a consequence of the virtualization of the network through Software Defined Networking (SDN) or Network Function Virtualization (NFV) technologies is the augmentation of possible transborder data transfer. In fact, Internet has no borders, and an unwanted transborder data transfer can happen if the network slicing service provider is located outside the country or the European Union. In addition, the complexity brought by the SDN/NFV technologies is illustrated by the different kinds of components in the 5G infrastructure architecture. These components can be hosted in different locations in the different contexts defined in the global 5G architecture: cloud, edge. There are different types of data controllers or owners, thus all the actors must comply to the regulations and laws applied in their country and some differences can be observed between countries with unwanted side effects on the data ownership. The 5G network slicing is intended to create end-to-end (E2E) communications in the global mobile network. The data is transferred between several components and eventually, services that are managed by different actors implementing different regulations and good practices. As the actors working in the different parts of the 5G infrastructure are heterogeneous and have different business objectives at the end, the application of the security and privacy recommendations or good practices can be slightly different from an actor to another one. These differences could create weak points in the complete chain of data transmissions among the components of the 5G infrastructure. Apart from that, there is also an infrastructure control concern. An important shift in the 5G paradigm compared to older telecommunication technologies is the fact that the telecommunication operators are giving a part of their control to new network slicing service providers.

Having conducted a contextual overview of privacy and security issues related to Network Slicing (such as securing the IP layer, data localization, stable cross-border transfers, data ownership determination, infrastructure control, security level standardization, and data confidentiality assurance), the key outcome of this task was the proposal of both technical and organizational solutions for privacy and security. From a technical perspective, innovative SDN-based pseudonym changing strategy is proposed to support both infrastructure and infrastructure-less vehicular zones:

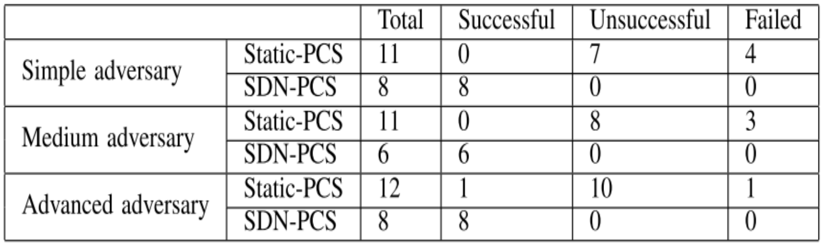
1. Situation-centric and dynamic pseudonym changing strategy for SDN-based 5G Vehicular Networks

The standardized approach to ensure location privacy in vehicular networks is the frequent changing of pseudonyms. In this context, many pseudonym changing strategies have been proposed. However, most of the proposed strategies are static, rigid and not adapted to the context. To overcome this limit, we have proposed a new SDN-based Pseudonym Changing Strategy (PCS). This strategy uses SDN controllers as the strategy coordinators and relies on them to change the security parameters of pseudonym changing strategy. This proposed strategy supports both infrastructure and infrastructure-less vehicular zones.

Key results



(a) Simple adversary. (b) Medium adversary. (c) Advanced adversary.



		Total	Successful	Unsuccessful	Failed
Simple adversary	Static-PCS	11	0	7	4
	SDN-PCS	8	8	0	0
Medium adversary	Static-PCS	11	0	8	3
	SDN-PCS	6	6	0	0
Advanced adversary	Static-PCS	12	1	10	1
	SDN-PCS	8	8	0	0

This strategy:

- Optimizes the number of Pseudonym changing Processes PCPs to be executed

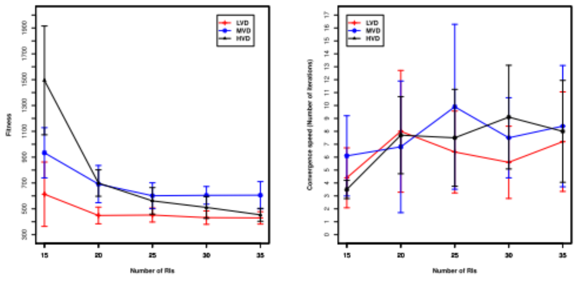
- The average response time is improved by more than 38% when using SDN-PCS.

- Causes less overhead in terms of messages than static PCS (54% of messages are saved)

2) Privacy-by-design approach for SDN-based 5G Vehicular Networks

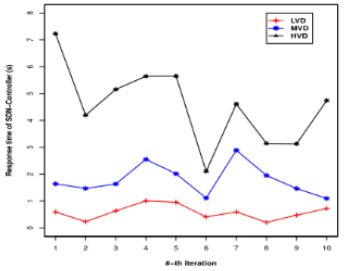
Vehicular Location Privacy Zones (VLPZs) is a promising approach to ensure unlikability. These logical zones can be easily deployed over Roadside infrastructures (RIs) such as gas stations or electric charging stations. However, the placement optimization problem of VLPZs is NP-hard and thus an efficient allocation of VLPZs to these RIs is needed to avoid their overload and the degradation of the QoS provided within theses RIs. This work considers the optimal placement of the VLPZs and proposes a genetic-based algorithm in a software defined vehicular network to ensure minimized trajectory cost of involved vehicles and hence less consumption of their pseudonyms.

Key results



(a) Fitness. (b) Convergence speed.

- This approach is cost-efficient and ensures a shorter response time.
- Fitness decreases gradually when the number of RIs increases.



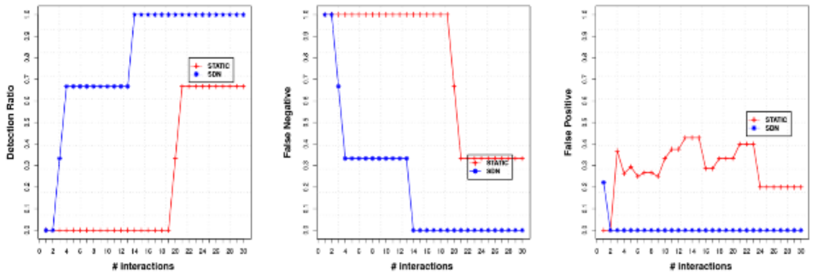
- Fitness values keep for low and medium vehicular densities and are enhanced in high density.

- The convergence speeds under different vehicle densities are close when the number of RIs is max.

3) Situation-centric and dynamic misbehavior detection system for SDN-based 5G Vehicular Networks

Vehicular networks are vulnerable to a variety of internal attacks. Misbehavior Detection Systems (MDS) are preferred over the cryptography solutions to detect such attacks. However, the existing misbehavior detection systems are static and do not adapt to the context of vehicles. To this end, we exploit the Software-Defined Networking (SDN) paradigm to propose a context-aware MDS. Based on the context, our proposed system can tune security parameters to provide accurate detection with low false positives.

Key results



(a) Detection ratio (b) False negative (a) False positive

	Size of Cluster	Ratio of misbehaving Vehicles	nbr_w	σ	γ
Context 1	20	10%	1	0.55	1.5
Context 2		30%	1	0.6	1
Context 3	30	10%	1	0.67	1.5
Context 4		30%	1	0.7	1.5

- The system is Sybil attack-resistant and compliant with vehicular privacy standards.

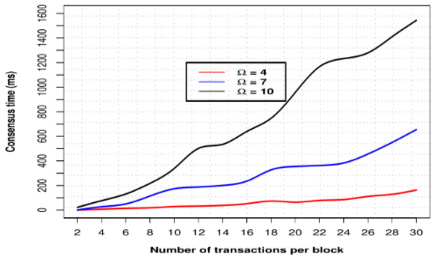
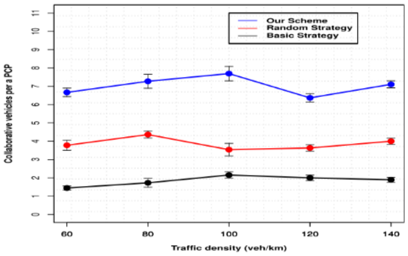
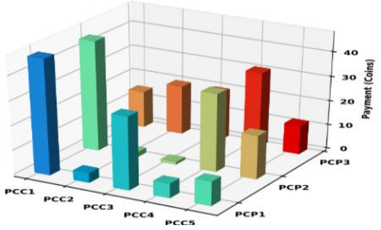
- Under different contexts, our system provides a high detection ratio and low false positives compared to a static MDS.

4) Blockchain for cooperative location privacy preservation in 5G-enabled Vehicular Fog Computing

Cooperation between vehicles is mandatory for achieving location privacy preservation. However, non-cooperative vehicles can be a big issue to achieve this objective. To this end, we propose a novel monetary incentive scheme for cooperative location privacy preservation in 5G-enabled Vehicular Fog Computing. This scheme leverages a consortium blockchain-enabled fog layer and smart contracts to ensure a trusted and secure cooperative Pseudonym Changing Processes (PCPs). We also propose optimized smart contracts to reduce the monetary costs of vehicles while providing more location privacy preservation.

Moreover, a resilient and lightweight Utility-based Delegated Byzantine Fault Tolerance (U-DBFT) consensus protocol is proposed to ensure fast and reliable block mining and validation.

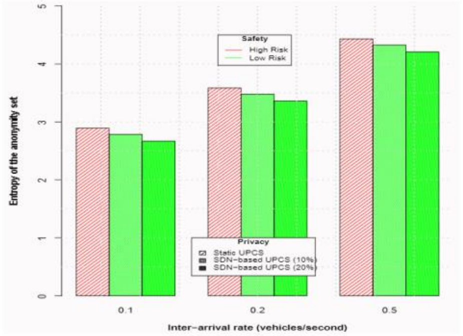
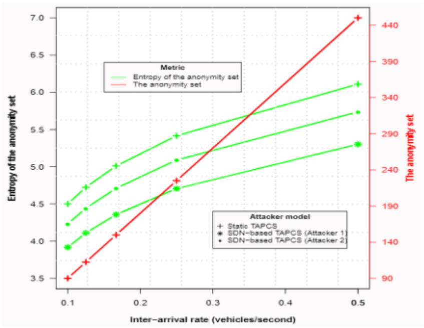
Key results

<table>
<tr>
<td>
</td>
<td>
</td>
<td rowspan="2">This scheme:
- Has effective incentive techniques to stimulate non-cooperative vehicles
- Provides optimal monetary cost management
- Provides secure, private, fast validation of blocks.</td>
</tr>
<tr>
<td colspan="2">
</td>
</tr>
</table>

5) SDN-based privacy protection framework for 5G Vehicular Networks

Software Defined Networking (SDN) is emerging as a key 5G enabler to manage the network in a dynamic manner. SDN-enabled wireless networks are opening up new programmable and highly-flexible privacy-aware solutions. We exploit this paradigm to propose an innovative software-defined location privacy architecture for vehicular networks. The proposed architecture is context-aware, programmable, extensible, and able to encompass all existing and future pseudonym-changing strategies (PCSs). To demonstrate the merit of our architecture, we consider a case study that involves four pseudonym-changing strategies, which we deploy over our architecture and compare with their static implementations.

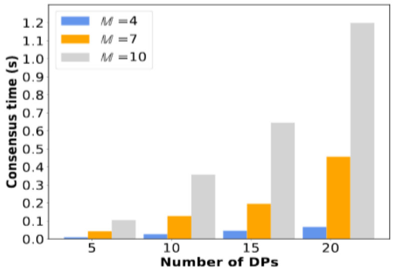
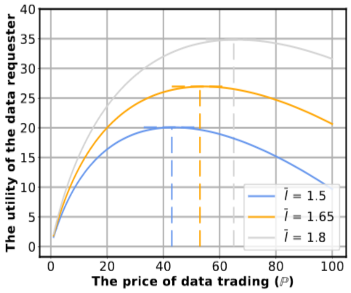
Key results

<table>
<tr>
<td>
</td>
<td>
</td>
<td>The proposed architecture is flexible and self-adapts to PCSs proposed far in the literature.</td>
</tr>
</table>

6) Blockchain-SDN based data trading scheme in 5G Vehicular Fog Computing

The size and variety of data collected by connected vehicles have enabled new data trading business models. However, lack of trust, scalability, privacy, and flexibility are among the main obstacles to build successful vehicular data trading services. In this solution, we leverage Software-Defined Networking (SDN) and blockchain to propose a novel scalable and secure data trading scheme for 5G enabled Vehicular Fog Computing. The scheme's blockchain system consists of SDN controllers, which relies on a resilient and lightweight consensus protocol to ensure fast and reliable block mining and validation. We design a secure and fair data trading smart contract between data requesters (vehicles) and data providers (vehicles). We also combine the SDN and a genetic algorithm for dynamic and context-aware placement of fog stations. Moreover, we analyze the scheme's fairness and monetary incentives based on the Stackelberg game model.

Key results

		This scheme provides: - Effective and efficient data trading. - Secure, private, and fast validation of blocks -Optimal and fair monetary price management.

E) Proposed Organizational Solutions:

As an organizational solution, the use of personal data protection certifications is explored for addressing the lack of harmonization between various jurisdictions and standard requirements, analyzing the value-added contribution of the Europrivacy™/® Certification Scheme.

Developed through the Horizon 2020 research programme, Europrivacy has been designed to encompass the whole range of requirements found in the GDPR and can easily be extended to include complementary national and domain-specific obligations, which makes it particularly relevant in the context of 5G-DRIVE. It has been designed to be comprehensive and capable of assessing a large scope of data processing activities by complementing its core list of checks and controls with complementary ones according to the Target of Evaluation. While its focus is on data processing activities (following the required approach by EDPB), its dual compliance with ISO/IEC 17065 and 17021-1 (where applicable) enables Europrivacy to assess data processing in the context of services, products, processes, and information management systems.

It has been designed to deliver homogeneous, consistent, and reliable certifications applicable to diverse categories of data processing activities. Beyond the core GDPR requirements, Targets of Evaluation may be subject to complementary national regulations. Particular application domains and technologies may also expose the data subjects to specific risks for their rights and freedoms. Consequently, Europrivacy is structured in a sequence of complementary criteria, checks and controls, including:

- **The Europrivacy GDPR Core Criteria**: which gathers the common criteria for assessing compliance with the GDPR requirements. They are mandatory and applicable to all data processing.

Europrivacy also considers three sets of complementary requirements, namely:

- **Complementary Contextual Checks and Controls**: to assess compliance with the domain- and technology-specific requirements. It enables to address technology- and domain- specific risks for the data subjects.
- **Technical and Organizational Measures Checks and Controls**: to assess the security measures set in place to protect the processed data.
- **National Data Protection Obligations**: with their complementary data protection requirements.

A key objective of the Europrivacy criteria is to reduce the risk of subjective interpretation by the auditor. It is important to prevent the risk that two auditors certifying the same data processing may reach different conclusions.

In summary, all Europrivacy certifications must comply with a set of Core GDPR Criteria, which encompass the core obligations of the GDPR applicable to all data processing. Additionally, the auditor must apply complementary criteria to assess the requirements associated with specific technologies or application domains that are present in the Target of Evaluation. These domains- and technology-specific complementary criteria can be extended to address new technologies and jurisdictions.

Following continuous discussions with the ECCP, the 5G-DRIVE project was invited to specify a set of conformity assessment criteria, which has been submitted for evaluation by the Europrivacy International Board of Experts. Upon its approval as Europrivacy complementary checks and controls, they will be submitted to the Luxembourgish Data Protection Authority for review and posterior submission to the European Data Protection Board with the goal of ensuring their widespread adoption. The resulting extension to the Certification Scheme provides several benefits to organizations involved in the development of connected vehicles worldwide, as it will provide a streamlined and interoperable avenue to demonstrate compliance with personal data protection requirements of both Europe and other jurisdictions, simplifying the process for market entry and raising the potential of adoption of new technologies by enhancing end-user trust in innovative data processing activities.

To define a new criterion, a systematic process must be followed that considers both the above-mentioned principles, as well as formatting requirements, avoiding any ambiguity. Criteria are overviewed by the Europrivacy International Board of Experts and are regularly updated to consider the evolution of the jurisprudence and the publications of the EDPB. In this context, the process of proposing technology-specific criteria extensions as undertaken by 5G-DRIVE must consider not only the state of the art on the relevant technology, but also ensuring an adequate balancing of efficiency and demonstration of compliance with the highest identified data protection requirements (e.g.: whenever incorporating nationally or sectorially defined requirements, developed criteria should not decrease the level of protection defined by the GDPR, and may raise this level if appropriate vis-à-vis the aforementioned principles of criteria specification).

The process for the generation of the technology-specific extensions to the Europrivacy Certification Scheme for connected vehicles was performed in two stages. The first stage of the process was to identify relevant documents containing specific information and legal requirements for the connected vehicle industry with the focus on data protection and data privacy. Secondly, the assessment examined the work of national data protection supervisory authorities of all Member States of the European Union, on how to address the initial inconsistencies and legal challenges of the connected vehicle industry. Finally, the assessment also studied the findings and proposals of national associations of the automotive industry, particularly those who have submitted codes of conduct and best practices on relevant topics for their consideration and approval by national supervisory authorities. Once this preparatory phase was concluded, an in-depth analysis was carried out to determine the obligations and specifications mentioned by the documents.

This process took place in several iterations, where requirements were extracted, compiled, and synthetized to properly convey the necessary information. It concluded with the adaptation of the draft criteria to match the Europrivacy guidelines on criteria generation with the final goal of easing their adoption by the International Board of Experts. The final list of proposed criteria addresses the following topics:

1) Enabling personal data protection safeguards by default
2) Identification of data categories
3) Data management / data subject right compliance
4) Data retention compliance
5) Data breach information
6) Update and review of privacy measures
7) Data processing information or documentation
8) Vehicle usage data communication
9) Regular processing of geolocation data
10) Special processing of geolocation data in case of theft
11) Tracking via in-vehicle WiFi technology
12) In-car applications and processing
13) Behavioral monitoring
14) Utilization of requirements for eCall system
15) Securing vehicle’s communications
16) Other security measures
17) Biometric data restrictions
18) Data processing revealing criminal offences or other infractions
19) Protection of traffic and communication data

As the draft criteria have yet to be approved by the EDPB, 5G-Drive T5.4 will continue to address any request for modifications and updates until the end of the project and will perform a final validation of the expressed criteria through bilateral calls with consortium members before the project finalization, with the end-goal of showcasing project results and easing the implementation of this solution in real-world deployments.

Conclusions

The work performed by 5G-DRIVE T5.4 enabled the identification of contextual, technical, and legal challenges of relevance for future 5G vehicular networks. As a result of this process, a number of technical solutions were proposed, including a situation-centric and dynamic pseudonym changing strategy; a privacy-by-design approach; a situation-centric and dynamic misbehaviour detection system; a SDN-Based privacy protection framework for 5G vehicular networks; a blockchain for cooperative location privacy preservation, and a blockchain-SDN based architecture for 5G-enabled vehicular fog computing. These technical solutions were complemented with an organizational view to address the remaining gaps between legal frameworks. To this end, the task proposed the use of interoperable and voluntary personal data protection certifications enabled by GDPR Art. 42 and supported by existing certification frameworks in both relevant jurisdictions. To ensure the relevance of this potential solution, the task proposed an extension of the criteria used by the Europrivacy Certification Scheme which is focused particularly on Connected Vehicles.

The adoption of the proposed technical and organizational solutions by the industry could help enhancing trust and demonstrating compliance across various global stakeholders, thus increasing trust, security and personal data protection in the connected vehicle ecosystem and in future 5G vehicular networks.