Privacy by Design Aspects of C-V2X

5GAA Automotive Association

White Paper

CONTACT INFORMATION:
Lead Coordinator – Thomas Linget
Email: liaison@5gaa.org

MAILING ADDRESS:
5GAA c/o MCI Munich
Neumarkter Str. 21
81673 München, Germany
www.5gaa.org

VERSION:	1.0
DATE OF PUBLICATION:	28/10/2020
DOCUMENT TYPE:	White Paper
EXTERNAL PUBLICATION:	Yes
DATE OF APPROVAL BY 5GAA BOARD:	08/10/2020

Contents

Contents

Privacy by Design Aspects of C-V2X

Connected vehicles, as part of the emerging Cooperative Intelligent Transportation Systems (C-ITS) are positioned to transform the future of mobility – a change enabled by the exchange of messages between vehicles and between vehicles and transport infrastructure. As these messages are constantly broadcasting data, including vehicle speed and location, this raises potential concern about how to address privacy and data protection.
In this document, we take a fresh look at the latest technological architectures that feature Privacy by Design. We focus specifically on Cooperative Awareness Messages (CAM) and Decentralised Environmental Notification Messages (DENM), where privacy protection is offered by using pseudonym certificates that do not contain any identifying information.
A Public Key Infrastructure (PKI) system takes care of the provision and overall management of the corresponding cryptographic keys. In this document, we review how current PKI system design can help address the risk of tracking from outside and inside attackers, and we identify challenges and privacy risks that remain unresolved. We give some suggestions in terms of future research and conclude the document with general recommendations.

1. The Purpose and Importance of V2X Communications

Vehicular-to-everything (V2X) communication encompasses vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) messaging. V2X communication systems are expected to greatly improve road safety and traffic efficiency while better supporting autonomous driving. V2X promises to save lives directly by providing road hazard warnings to the driver and reducing collisions. The efficacy of V2X, however, is directly correlated to its adoption; the more vehicles enabled with V2X, the safer our roadways will be (and vice-versa). It is therefore of critical importance that V2X respects privacy in its design, not merely as a matter of legal compliance, but also to ensure consumer trust and mass adoption.

2. Privacy in V2X Communications

V2X applications rely on continuous and detailed location information, which may raise privacy concerns. For privately owned vehicles, location traces would, if accessed, reveal the movements and activities of its driver, who may not necessarily be the owner of the vehicle. So, sending and disseminating V2X user location information can be considered a potential privacy concern for both the owner and the driver of the vehicle.

V2X safety messages can include a Cooperative Awareness Messages (CAM), a Decentralised Environmental Notification Messages (DENM) or a Basic Safety Message (BSM). The CAM and DENM can be used in European (EU) standards and the BSM in United States (US) standards. CAM messages are broadcasted quasi-continuously (at 1-10 Hz) and they contain kinematic data, as well as the dimensions of the vehicle. DENM messages are broadcasted in addition to the CAM messages, but only upon the occurrence of specific events (i.e. accidents) or in urgent situations, and they contain geolocation information about the event. The BSM can be both a periodic broadcast and triggered by events. For the sake of simplicity, in what follows we will restrict ourselves only to the European standard messages (CAM and DENM), but the same holds for BSM as well.

This document addresses privacy issues arising from attacks primarily concerned with the short-range broadcast of V2X messages. Yet such data is also used by trusted back-ends, including Original Equipment Makers (OEMs), Road Operators, and other stakeholders, so presumably in such a case the messages have been captured and backhauled to the back-end for legitimate reasons.

Indeed, depending on how the services are realised, the potential privacy implications may differ. If information is filtered, anonymised and potentially aggregated (for anonymity and quality of data purposes) by trusted back-end systems before being shared with other actors, the privacy risks can potentially be mitigated. So, with the right privacy protection mechanisms in place, the vehicle OEM back-end can process geolocation data and disseminate relevant information to the vehicles concerned. The concept of exchanging information between back-end systems is in place for several vehicle manufacturers, and it is also emerging in a number of projects that aim to include Road Authorities/Road Operators and other actors in the ecosystem, e.g. in the Nordic Way Solution [1], and it is also being put forward by the EU C-Roads project as part of the 'Specification for interoperability of back-end hybrid C-ITS communication' [2] and future C-Roads releases.

However, as we noted, this white paper addresses the privacy considerations when using short-range broadcast technology (PC5 and 802.11p) where the receiver can be anybody. Without specialised equipment, such as directional antennas, CAM and DENM messages can be detected up to about a kilometre from the transmitting vehicle under good conditions (unobstructed lines of reception and few other transmitters), and up to 300 m from the transmitting vehicles in congested situations, depending on environmental conditions. This short-range nature of the broadcast is important in order to define the attacker model and privacy protection mechanisms, as we will outline in the following subsections.

In recent years, several legislative initiatives on data protection and data privacy have been adopted by national or regional governments, amid growing public concerns. The most prominent initiative to date is arguably the EU General Data Protection Regulation (GDPR, Regulation (EU) 2016/679), or the ePrivacy Directive (Directive 2002/58/EC), which is currently under revision. While taking stock of this state of play and related literature, this document does not address legal aspects nor constitute a 5GAA position on this matter: it focuses only on technological architectures to ensure Privacy by Design.

2.1 Content of CAM and DENM Messages

We will now take a closer look at the contents of CAM and DENM messages. Figure 1 illustrates the structure of Cooperative Awareness Messages, which are comparable to beacon messages. They are broadcasted periodically with a packet generation rate of 1-10 Hz. A CAM reveals a lot of dynamic information about the associated ITS vehicle station: geographic position, speed, driving direction, etc. at a specific time [3]. In addition, static information, e.g. the confidence levels of heading, speed, acceleration, curvature and yaw rate, and the length and width of the ITS vehicle station are given. To assure message integrity and authenticity, CAMs contain an electronic signature and the appropriate certificate. It is not planned to forward CAM messages hop-by-hop, while at the same time forwarding is not technically prevented either.

Figure 1: Structure of a CAM message

Header	Signer_Info
	Generation_Time
	ITS-AID for CAM
CAM Information	ITS-Station Type
	Last Geographic Position
	Speed
	Driving Direction
	Longitudinal Acceleration
	Curvature
	Vehicle Length
	Vehicle Width
	Steering Angle
	Lane Number
	...
	Vehicle Role
	Lights
	Trajectory
	Emergency
	Police
	Fire Service
	Road Works
	Dangerous Goods
	Safety Car
	...
Signature	ECDSA Signature of this Message
Certificate	According Certificate for Signature Verification

In contrast, the second message type, Decentralised Environmental Notification Messages, are event-driven and indicate a specific safety situation. The DENM message format is detailed in [4] and can be transmitted hop-by-hop. Figure 2 illustrates the structure of a DENM message.

Figure 2: Structure of a DENM message

Header	Signer_Info
	Generation_Time
	ITS-AID for CAM
DENM Information	Last Vehicle Position (GPS)
	Event Identifier
	Time of Detection
	Time of Message Transmission
	Event Position (GPS)
	Validity Period
	Station Type (motorcycle, vehicle, truck)
	Message Update/Removal
	Relevant Local Message Area (geographic)
	Traffic Direction (forward, backwards, both)
	Transmission Interval
	...
	Information Quality (low-high)
	Event Type (number)
	Linked Events
	Event Route (geographical)
	Event Path
	Event Speed
	Event Direction
	Road Type
	Road Works (speed limits, lane blockage,...)
	...
Signature	ECDSA Signature of this Message
Certificate	According Certificate for Signature Verification

2.2 Privacy by Design of CAM and DENM Messages

The accuracy and reliability of V2X safety messages (i.e. integrity) are of prime importance because they have direct impact on the safety applications' effectiveness. Secure V2X communication is thus paramount. Digital certificates to authenticate messages in vehicular communications are used to prevent an attacker from injecting false messages [5]. The distribution of certificates among the peers is made using the Public Key Infrastructure architecture.

In V2X communication, the actual identity of the sender is not required to ensure the trustworthiness of a message. It is sufficient to verify that a message has been sent by a valid V2X participant. To further avoid identifying the individual broadcasted V2X messages, it is suggested that the certificate should not contain any information that links them to a particular vehicle or driver, in order to protect the privacy of individuals. Instead, vehicles are assigned multiple pseudonym certificates, which reduce the chance of re-identification [6].

However, this is not enough to offer geolocation privacy. An attacker who is able to link several messages together over time and concatenate the geolocation information, could easily build geolocation profiles and relate them to a specific vehicle. This can be done by using additional information obtained via cameras or correlating profiles to specific areas. For example, if a geolocation profile starts and ends at the same locations, this may reveal home and work addresses that could then be connected to individuals [7].

More specifically, if a vehicle uses a single pseudonym certificate through its lifetime, then this enables an attacker, who observes the certificate at different locations, to link the CAM messages. So a vehicle needs to change between multiple pseudonym certificates that are cryptographically 'unlinkable' to each other. Each vehicle uses a pseudonym certificate to sign CAM and DENM messages for a limited period of time before being changed. In this way, we make it harder for attackers to link messages together and profile vehicles as broadcasting stations based on location traces. We define this more formally in the next section.

2.3 Privacy Requirements

As soon as the data leave the vehicle, appropriate precautions must be taken to ensure lawful processing of any personal data. At present, there is uncertainty among stakeholders on how to comply with data protection requirements in the context of V2X communications. Some initiatives at the European level attempted to investigate these issues.

The Data Protection Working Group of the C-ITS Platform [8] led one of the first analyses of privacy and data protection issues to achieve a seamless and harmonised introduction of C-ITS in the European Union. In its final report, the group concluded that "the preferred solution in the long term should be based on a legal obligation where the processing of data is necessary for the performance of a task carried out in the public interest"[1]. In September 2017, the International Conference of Data Protection and Privacy Commissioners (ICDPPC) adopted a resolution on connected vehicles [9], and in October 2017, the Article 29 Data Protection Working Party adopted an Opinion regarding the processing of personal data in the context of C-ITS [10].

While the above initiatives have brought attention to the legal discussion, there still needs to be a clear understanding on how to comply with rules on the privacy and protection of personal data in the context of C-ITS, especially for safety-related applications where benefits cannot be generated unless the data is shared. It is of utmost importance that we guarantee continuity of safety-critical services to EU drivers and, thereby, comply with related EU regulations in place.

Notwithstanding the outcome of the legal interpretation of privacy requirements, any V2X communication system should incorporate technical means to protect privacy in its design. We can translate this into a list of identified requirements, as follows (see also [11] for additional details on privacy requirements):

Minimum disclosure: The amount of information revealed by a user in a communication should be kept to the minimum and should be not more than what is required for the normal operation of the system.

Conditional Anonymity: Individual vehicles should be anonymous within a set of potential participants. If a vehicle deviates from system policies, the corresponding long-term identity can be retrieved by the PKI entities, and revoked temporarily or on a permanent basis [12].

Unlinkability: To achieve this, no entity should be able to link the different pseudonyms of a specific vehicle with each other.

Forward and backward privacy: The revocation of a credential does not affect the unlinkability of previously signed messages. Also, if an attacker recovers the identity of the sender of a particular credential, it should not affect the privacy of other messages signed by the same sender.

1. C-ITS Platform Final Report Phase II (September 2017)
https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf

2.4 Attacker Model

Since the vehicular network is a complex distributed system, there are several kinds of attack that a stakeholder or an individual can perform for legitimate or **illegitimate** purposes. To understand the countermeasures built into the system, it is useful to understand how such a stakeholder would actually track an individual. The steps are as follow:

1. Record messages across multiple locations
2. Determine that some set of messages spread across those locations have come from the same vehicle
3. Link the messages to an individual (or link the location traces obtained in step 1 and 2 to an individual)

Let us look more analytically at the steps above. How realistic would it be in step 1 to record messages in multiple locations? Studies indicate that the cost of setting up a message-recording network would be beyond the capabilities of most individuals, though not for an organisation of reasonable size [6]. The system design therefore does not assume that the attacker is significantly constrained in how they can 'sniff' the network. Likewise, the amount of data produced by vehicles in the V2V system is enormous – 2 kilobytes per vehicle per second[2] or over a terabyte an hour in an area with a million vehicles. This volume may put off an unsophisticated attacker, but a sophisticated attack can pre-process data before storing it (by stripping off security headers, only storing significant changes in direction or speed, etc.), and so the design does not assume that data storage is a significant constraint. However, the design does implicitly assume that there will be at least some areas where an attacker will not be recording at any particular time. It is thus assumed that this kind of snooping by non-law-enforcement organisations will be illegal, and so anyone carrying out this kind of activity will want to balance their ability to track individuals against the risk of getting caught.

So, the assumption is that a stakeholder cannot record all messages, but will have gaps in their coverage. This prevents them from joining the dots on received messages to reconstruct a vehicle's entire route. Instead, they could choose to target a particular route through a particular area. There is ongoing academic research into ways to periodically disrupt tracking, even in locations where an entity is actively listening, while not impacting the safety mission of the system. This research is promising but not currently widely accepted.

[2] This is based on ten Basic Safety Messages per second, each of which is about 200 bytes long.

Regarding step 2, a stakeholder could link messages to the same vehicle if one of the following holds:

1. The messages all explicitly identify the vehicle (or the driver)
2. The messages all contain some data which is unique to that vehicle (or sent by very few vehicles – in this case the attacker can use data analysis mechanisms and guesswork to determine which vehicle sent which message)
3. The vehicle radio transmissions have some physical (for example, radio frequency, RF, fingerprint or timing) characteristic that distinguish them from transmissions emanating from other vehicles
4. The attacker can observe a large number of transmissions from the vehicle and join the dots between them, determining the vehicle's path in real time

Finally, step 3 can be carried out in one of two ways:

1. Link the messages directly to an individual, or
2. Link the messages to a vehicle, for example by observing the vehicle and simultaneously recording a message that identifies its location, and then link the vehicle to an individual

We differentiate between the following attacker models [13]:

Inside attacker: An inside attacker is one who has access to any PKI component. It is assumed that the attacker does not maliciously destroy data but only eavesdrops or processes data for a gain, such as a legitimate insider (e.g. law enforcement), or in the case of a hacker, to gain sensitive information, or a rogue employee. This attached model requires mechanisms to counter inside attackers via technical means, hence it is a stronger than the usual assumption of a secure PKI via organisational means.

External attacker: An external attacker can listen on over-the-air V2X communication or physically compromise V2X units. The attacker is sophisticated and able to remove components from vehicles, open units, run side-channel attacks, etc. This is a standard attacker model assumption.

One could also differentiate between global and local attackers [14]; a local attacker is limited in scope, even if the attacker has control of several vehicles or base stations. A global attacker has an extended scope controlling entities scattered across the network. However, global attackers are explicitly excluded from our attacker model [13], because it is not realistic to consider that a large, well-funded entity would deploy a comprehensive network of road-side units for tracking purposes. Indeed, the Car-2-Car Communication Consortium (C2C-CC) notes that: "The threat scenario of ubiquitous eavesdropping is deemed as not probable (i.e. probability ~0) unless an illegitimate controller (i.e. an unofficial or unlawful organisation – in C-ITS terms) can be demonstrated to have both the resources and the interest to build up a ubiquitous network to survey an area of interest such as a region or city." [15]

2.5 Technical Requirements

First, we need to clarify that a degree of short-range tracking is necessary to enable V2X applications, since it allows for the connection between road conditions and the vehicles driving in the area [16]. Protecting location privacy of individuals is about preventing long-term tracking that is not essential for road safety.

Second, we need to make clear that in order to satisfy the privacy requirements outlined above, we need to make sure that CAM and DENM messages cannot be linked by using information in any of the layers involved. In order to satisfy this requirement, several technical parameters should be taken into consideration:

1. **No explicit identification:** The messages do not contain an 'explicit identifier' – e.g. a vehicle identification number (VIN), driver's licence number, home address, insurance policy number, parts serial number, etc. – at the level of the onboard unit (OBU), vehicle, or driver.
2. **Pseudo-identifiers are temporary:** The messages include several fields that are unique, or locally unique, to the sender. These include, non-exhaustively:
   - Temporary ID in the application payload
   - Security certificate in the security envelope for the application payload
   - Source IP address if the message is sent over IP

These fields are referred to below as 'pseudo-identifiers' because, while they don't contain real-world identification information, they are unique in the vicinity of the sending vehicle and so can be used to determine which sets of messages have been sent from specific vehicles.

In the design, all pseudo-identifiers are temporary. The Car-2-Car Communications Consortium has proposed mechanisms to determine when a pseudo-identifier set change is to occur [15]. At this point, the vehicle briefly stops generating new messages and flushes the message queues. Once the message queues are flushed, the OBU starts generating new messages again, but with all the pseudo-identifiers changed. This means that an eavesdropper who does not overhear the messages sent at the exact time of the change is significantly hampered in their ability to match messages occurring after the change to those from before the change. Further subtleties of this approach are discussed below.

3. **Vehicle identifying information is coarse**: The messages also contain information like vehicle dimensions and weight. If this were given to the nearest centimetre it would act as a pseudo-identifier, distinguishing each vehicle from basically all vehicles of other makes and models. However, the granularity of the information is coarse – 10 cm precision or more – meaning that the set of vehicles with the same characteristics is relatively large.
4. **Transmission behaviour changes when pseudo-identifiers change:** The fundamental system concept is that, when channel conditions allow, each vehicle broadcasts awareness messages ten times a second. In order to

prevent simultaneous transmissions by multiple vehicles, they might choose a timeslot within each 100-millisecond interval to carry out transmissions. This approach is not required under the current standards, but has been adopted in practice in many deployments. In this case, the offset time into each 100-millisecond interval is also a persistent characteristic of the OBU. In order to prevent this being used for tracking, the offset time is randomised when the message changes its pseudo-identifiers [17].

5. **RF fingerprinting is not a significant attack vector:** Research has been carried out into the ability to track devices by their 'RF fingerprint', i.e. characteristics of how they carry out transmissions [18]. Although it has been determined that commercial-grade radios typically do have some unique characteristics making it possible to distinguish them from other radios in the same type of device (i.e. in principle you can tell one OBU from another), in practice this is not considered a unique threat caused by the V2X system for three reasons:

   - First, it needs more sophisticated receiving equipment than would be required for tracking based on data fields, and so is beyond the capability of many attackers.
   - Second, in order to determine the characteristics of a radio enough to be useful for tracking, an attacker must observe the radio for some period of time in a relatively clean RF environment; an attacker capable of this could mount other attacks, such as attaching a tracking device to the car. This also means that an attacker who wants to use this approach must select in advance the OBU they want to track, which means that they cannot carry out a mass 'fishing expedition' that compromises privacy on a grand scale.

Lastly, RF fingerprinting works against all RF devices, including mobile phones, and so V2V does not introduce any new, unique, or significant additional risk from RF fingerprinting and tracking compared to the existing situation.

So, in this document we focus mainly on the impact that the privacy requirements have on the certificates attached inside CAM and DENM messages. More specifically, we have mentioned that vehicles use several pseudonym certificates which are interchanged over time in order to avoid tracking. Here, we express this in more concrete terms:

- A pseudonym has to be used for a limited time
- A pseudonym has to be unique, meaning that no other vehicle can use the same one
- A new pseudonym must always be available for the vehicle to enable the pseudonym change [19]

In addition, any pseudonym certificate provisioning system that will be used to secure V2X communications should satisfy the following constraints:

- The system must scale to support a large number of vehicles
- The system must be fast to support critical application like collision-avoidance; that is, communication exchange should not be burdened by the security overhead
- The system must operate in a highly mobile environment, where there may be only sporadic availability of the communication channel between the car, road infrastructure and back-end infrastructure
- The system must support revocation of misbehaving vehicles

So, now we can revisit the privacy requirements first presented in Section 2.3 and map them to the technical requirements presented in this section, as illustrated in Table 1.

Table 1: Mapping of the privacy requirement to controls and technical requirements

Privacy Requirement	Controls – Technical Requirements
Minimum disclosure	No explicit identification. Pseudo-identifiers are temporary. Vehicle identifying information (e.g. vehicle dimensions, etc.) is coarse.
Conditional anonymity	The system should be able to identify misbehaving vehicles and take corrective measures.
Unlinkability	Pseudonym changing properties: a pseudonym should be used for a limited time, and multiple pseudonyms should be available to a vehicle in order to enable pseudonym change. Transmission behaviour in lower layers should change when pseudo-identifiers change.
Forward and backward privacy	Supported by revocation mechanism: certificates for current and future time periods are revoked; messages signed in past time periods cannot be linked.

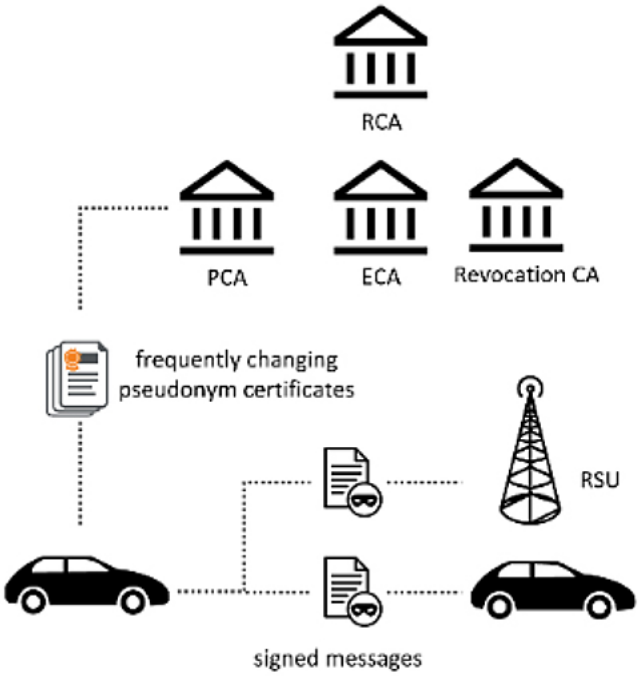
3. Certificates and Pseudo-Identifier Change

One significant pseudo-identifier for V2X messages is the digital certificate that it uses to digitally sign messages. Aiming to cope with the management of these certificates, many proposals have appeared in the literature for creating a Vehicular Public Key Infrastructure (VPKI) (for a survey, see [20]).

The evolution can be traced from the first vehicular communication security architecture [21] to the most recent architectures, notably the Security Credential Management System (SCMS) [22] by a consortia of vehicle OEMs and the US Department of Transport (USDOT), as well as the European Cooperative-ITS Certificate Management System (CCMS) developed by the European Committee for Standardisation (CEN) and European Telecommunications Standards Institute (ETSI), with support from the European Commission [23]. The E-Safety Vehicle Intrusion protected Applications (EVITA) project [24] developed a prototype for securing in-car networks, while the Secure Vehicle Communication (SeVeCom) [25] and Privacy Enabled Capability in Cooperative Systems and Safety Applications (PRECIOSA) [26] projects addressed the complex security and privacy challenges over the wireless channel. Most recent efforts, such as the Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) and COmmunication Network VEhicle Global Extension (CONVERGE) [27] projects, worked towards the implementation of a complete secure and privacy preserving subsystem that employs a Hardware Security Module. Looking more into the future developments of VPKI systems, 5GAA has evaluated the Security Credential Management System (SCMS) and the C-ITS Security Credential Management System(CCMS)system designs and we have concluded that they can be improved to take advantage of cellular connectivity. The effort to identify potential design simplifications in order to increase efficiency and harmonise technologies across regions has resulted in an updated system design for large-scale deployment and cross-regional interoperability called the Efficient Security Provisioning System (ESPS) [28].

Broadly speaking, in all of the above systems, privacy and cyber security features have been realised by defining the certificate and security policy based on PKI management and pseudonymising the messages.

Figure 3: A V2X security solution based on PKI



The question then is how to apply the pseudonyms to vehicles. In the PKI approach, a set of Certification Authorities (CAs) provide credentials to the vehicles. In the general case, there is a set of different authorities with distinct roles:

Root Certificate Authority (RCA): This entity is the 'trust anchor' of the PKI, responsible for issuing certificates to sub-CAs. The certificate of the RCA is signed by itself.

Enrolment Certification Authority (ECA): This entity is responsible for registering vehicles and issuing long-term certificates. Entities with enrolment certificates can then apply to other CAs for pseudonym certificates.

Pseudonym Certification Authority (PCA): This entity is responsible for issuing certificates that do not contain any identifying information.

Certificate Revocation CA: Responsible for issuing revocation lists applying to various certificates.

Private key material associated with pseudonym credentials should be stored securely within the vehicle and not extracted or transferred outside it. For this reason, the integration of Hardware Security Modules (HSM) or Tamper-Proof Devices (TPD) in vehicles has been proposed for secure key storage and management [29].

To enable the pseudonym changing scheme, vehicles will need a large set of pseudonym certificates stored in-situ and/or downloaded periodically from the back-end. Additionally, in order to prevent a compromised vehicle from sending messages signed with multiple different certificates (i.e. appearing to be multiple vehicles), the number of certificates issued to each vehicle is controlled, limiting each vehicle's scope to change and potentially forcing the re-use of certificates.

To mitigate this, C2C-CC has proposed that the number of certificates should be set between 60 and maximum 100 [30]. C2C-CC has also proposed a set of algorithms to be used to determine when to re-use certificates; for example, because an eavesdropper interested in a particular vehicle is likely to listen closely to the vehicle owner's home as well, any certificate that is used at the start of a particular trip (including close to home) should not be re-used for any purpose unless there is no alternative, while certificates that have only been used in the middle of a trip may be re-used more freely.

Lastly, there is a risk that the CA itself will keep a record of which certificates have been issued to which vehicle. The CA could determine this by the authentication information contained in the certificate request, or by side-channel data, such as certificate requests clustered within a certain timeframe, or from the same physical location, or all from the same vehicle. Even if the CA does not maliciously store this information for the purpose of tracking, the information could end up being used for other purposes, for example to enable audits which are typically required for CAs to ensure that they are following policy. The system should thus include several design features to mitigate these problems, such as the use of Web/NAT proxies to obscure the physical location of requests, and allowing OBUs to time the requests for certificates and avoid evident clustering (in Europe – the US/IEEE design has a different approach that completely eliminates the risk of timing clustering) [22].

3.1 Organisational Separation of Duties

As noted in Section 2.4, we need to protect not only against outside attackers, but also inside attackers. The changing pseudonyms approach addresses the challenge posed by outside attackers. In order to protect against inside attackers, we need additional measures. One common approach is to divide the PKI operations into its component parts, which establishes an organisational separation between them. That means, components of the architecture are managed by legally/administratively separate entities with distinct governance, such that none of them have the sufficient knowledge, information, or means to link short-term certificates to vehicles/drivers/owners.

The SCMS design accounts for outside and inside stakeholders introducing the 'no single entity' criterion for the certificate generation, meaning that architecture is designed such that at least two entities need to collude in order to compromise users' privacy, i.e. relate a pseudonym to a vehicle or two pseudonym certificates to the same vehicle, which would enable long-term driver tracking. Similarly, CCMS specifies different entities responsible for requesting authentication verification and pseudonym certificate issuance [31].

3.2 Revocation of Pseudonyms

Certificate revocation is a standard consideration for any PKI system. In case of misbehaviour, the wrongdoer can be evicted, i.e. prevented from further participation. The revocation of back-end entities can be done in standardised ways by adding the revoked certificates to a Certificate Revocation List (CRL), which is then published by the CA responsible for that trust domain. But for vehicles using short-lived pseudonym certificates, things are more complicated. If a vehicle possesses multiple certificates that are unlinkable, every single certificate needs to be put on the CRL, which would increase the bandwidth requirement to unfeasible levels.

In one approach advocated under CCMS, pseudonym certificates are not revoked, but rather only the long-term identity of the vehicle can be revoked. Then the vehicle can continue participating in the system until all of its existing pseudonym certificates expire, and it has to request a renewal of its certificates from the system using its enrolment certificate, which would be denied because the certificate is on an internal blacklist of revoked vehicles. However, this does not prevent the vehicle from misbehaving while using pseudonyms it already possesses.

Another approach, followed by SCMS, is to still use Certificate Revocation Lists (CRL) to revoke existing pseudonym certificates, and find ways to address the bandwidth problem. For example, Nowatkowski et al. [32] have shown that the CRL list may grow as much as 2.2 GB, depending on the policy for the number of pseudonyms carried by the vehicle. SCMS resolves this by including a linkage value to pseudonym certificates derived from cryptographic seed material. Publication of the seed is sufficient to revoke all certificates belonging to the revoked vehicle. For protection against insider attacks, the seed is the combination of two seed values produced by two Linkage Authorities (LAs). There are also alternative solutions suggested in the bibliography that resolve the aforementioned large CRL issue by leveraging encrypted pseudonyms during the provisioning process [33] [34]. In such approaches, the vehicle can only decrypt pseudonyms after receiving the encryption keys.

4. Technical Considerations

Current V2X communication standards and protocols consider Privacy by Design as a major requirement, yet several open issues need further consideration. In the following pages, we develop on these issues.

4.1 Integrity and Confidentiality

CAM and DENM messages are cryptographically signed by the sender using a pseudonym to guarantee that the message information is integrity-protected and authentic. The PKI system takes care of the provision and overall management of the corresponding cryptographic keys. The PKI also provides the possibility to revoke a participant from the system by refusing to issue new pseudonym certificates.

However, CAM and DENM messages are not cryptographically encrypted. Encryption is used only for communicating with Certification Authorities. The nature of exchanging messages between vehicles is many-to-many and receivers need to be able to process the messages without delays. If messages were encrypted, receivers would have to know the decryption key in advance. Given that the sender is not known in advance, it is not possible to use different keys for different transmitters. This means everyone would have to use the same key, which degrades security [15]. At the same time, using an encryption scheme would slow down the exchange of messages. Given the high frequency of these messages, there is no margin for such delays.

4.2 'No Single Entity' Requirement

The SCMS concept envisages a technical separation of capabilities between different PKI authorities to cope with internal attackers, ensuring that no single authority can relate two pseudonym certificates to the same vehicle. However, there is no restriction on multiple authorities being operated by one organisation. For example, USDOT describes the removal of certain organisational separations of SCMS functions, which may now reside in the same organisation, while the responsibility is passed onto a single governing entity, a 'SCMS Manager',which ultimately decides on the rules for governance/policy of separation [35]. Note that in that document the SCMS manager is expected to be an industry-wide coalition of stakeholders.

The 5GAA Security Working Group has pointed out that including Mobile Network Operators (MNO) in the ecosystem can further justify the shift of onus to the SCMS operator. In our recent white paper on Efficient Security Provisioning Systems (ESPS),

the Working Group has re-evaluated the results of the risk assessment [28]. To start with, it is noted that the MNOs are already established as trusted parties, operating under regulatory constraints. Thus, given their access to location-sensitive information, the level of privacy protection within the MNO reaches the required threshold for location-privacy protection within the overall V2X system, whether or not the MNO is actually participating in a given V2X communication. As a result, the protection of privacy sensitive information should shift from a technical and organisational solution to an SCMS operator-specific solution mediated through trusted MNOs.

This re-evaluation of the risk assessment allows for a variety of simplifications, including the merging of LAs (assuming there are LAs) or even avoiding LAs [36], removing the Location Obscurer Proxy (LOP), and organisational separation of individual components (by allowing a single legal/administrative entity to own/operate different components of the SCMS). Hence, shifting the onus to the SCMS operator is not necessarily a problem, providing the SCMS operator decides on the rules for governance and establishes appropriate policies that prevent, for example, one person from being able to access information from more than one component of the PKI. However, removing the 'no single entity' criterion could reintroduce the risk of vehicle tracking by combining entities like the RA/LAs. However, this overall increase in vehicle tracking risk is similar to the existing risk associated with cellular coverage, whereby the MNO has operational knowledge of the current radio network connection and location of subscribed devices even while in idle mode.

4.3 Security and Trust

In general, different parties or authorities inside the V2X PKI ecosystem can possibly collude together to compromise privacy and track a vehicle, even though corresponding polices are in place. A basic element of PKI is that all participants in the system need to trust that these entities are honest and don't collude with each other. So, how do we establish and maintain this federated trust? The typical solution uses audits as verification of the CA's standards of operational and technical security [37]. The CA declares its Certificate Policy (CP) or Certificate Practice Statement (CPS), as defined in RFC 3647 [38], and it conforms to the specifications therein on when and how an audit takes place, what is covered by an audit and who carries it out. However, collusion or security incidents affecting CAs have grown more frequent in recent times [39], so the existence of a PKI architecture does not guarantee per se that trust exists between the actors, thus additional measures are necessary to reinforce a 'scalable web' of trust [10].

4.4 Change of Pseudonyms

The PKI system provides the necessary pseudonym credentials to the vehicle, and enables the pseudonym changing mechanism. However, the pseudonym change strategy is still under discussion. In general, changing pseudonyms does not offer perfect privacy protection and the existing technical solutions have some drawbacks. For example, there are still ways for an eavesdropper to link messages signed under different pseudonyms, exploiting the circumstances under which vehicles change pseudonyms [40]:

- Based on the time of a transition, an attacker might be in a position to observe a particular pseudonym change, and associate the old and new identifiers [41] [42].
- The attacker uses the physical constraints of the road layout, velocity, and heading of a victim's vehicle to predict its trajectory and link pseudonyms [43] [44].

In addition to a PKI system to manage pseudonym certificates, technical measures addressing the problem of changing pseudonyms are needed. A recent technical report from ETSI describes the pseudonym changing strategies in the literature and identifies corresponding drawbacks. [45].

4.5 Anonymisation of Data

As mentioned in Section 1, road-side stations may store and relay data from CAM and DENM messages for later processing, such as for traffic management. This kind of data should be anonymised as soon as possible, and preferably immediately after collection [8]. The operators of road-side stations therefore have to implement additional algorithms for anonymising collected data – even that derived and correlated from other sources, such as traffic patterns, etc. – and managing re-identification risk. In April 2014, the Article 29 Working Party adopted the Opinion 05/2014 on Anonymisation Techniques, where it analysed the effectiveness and limits of existing anonymisation techniques and provided recommendations to handle these techniques by taking account of the residual risk of identification inherent in each of them [46]. Such algorithms are still not sufficiently elaborated and demonstrated for highly complex data, such as V2X messages. The location information contained inside the data, combined with the fact that they are broadcasted continuously over time, assigns a multidimensional time series nature to the data and makes the application of anonymisation algorithms more challenging.

4.6 Future Research

Although the current PKI systems provide a foundational set of cyber-security capabilities for C-V2X, future research should also be planned to identify novel methods for enhancing privacy and data protection in vehicle communication. Seeking to design secure privacy-preserving architectures for V2X systems comprising millions of autonomous vehicles, we have to deal with unresolved challenges raised in the previous section. Security, interoperability and connectivity in a dynamic network of vehicles, gateways, services and applications across operations, technology and information technology stakeholders demands a strategic rethinking of policies and processes in the context of cyber-security, privacy and trust. Along these lines, it is worth investigating how new technologies can be used to stimulate new VPKI architectures and evolutions in the future. For example, one approach is to use advanced solutions based on privacy-preserving Attribute-Based Credentials (privacy-ABCs) that allow vehicles to generate multiple pseudonyms locally, and no further interaction with the infrastructure is needed [47]. An experimental assessment of the performance of privacy-ABCs for vehicular ad hoc networks is presented by de Fuentes et al. [48]. Similarly, Whitefield et al. [49] advocate the use of Direct Anonymous Attestation (DAA) algorithms and trusted computing technologies as an enabler for more decentralised approaches, where trust is shifted from the back-end infrastructure to the edge [50]. More research is needed to come up with more scalable and decentralised solutions eliminating the need for trust built around ‘federated infrastructure’.

5. Recommendations

A critical part of any efforts to achieve consumer acceptance through public outreach will be assuring consumers that V2X technologies do not pose a significant threat to privacy and have been designed to help protect against vehicle tracking by any government or company participating in the ecosystem. Towards this end, we recommend the following steps to enhance privacy protection and minimise risks.

- This document has presented solutions that incorporate Privacy by Design principles (see Table 1). It is recommended to foster the principle of Privacy by Design as a core component in related business processes. Developers will need comprehensive and practical assistance at an early stage to deal with the respective data protection requirements.
- We emphasise the importance of conducting Privacy Impact Assessments. In particular, adequate documentation of the relevant processes described in Articles 30 and 35 of the GDPR – including obligations to carry out Data Protection Impact Assessments (DPIAPIA) for sensitive data processing procedures – should be considered. A DPIAPIA will capture and quantify all privacy risks and assess the performance of technical, physical and organisational controls designed to minimise such risks.
- We recommend data minimisation, a reductive approach to data collection, seeking to collect and maintain the minimum of data needed for a specified purpose.

6. References

[1]	"NordicWay2," [Online]. Available: https://www.nordicway.net/. [Accessed 4 November 2019].
[2]	"The C-Roads Platform publishes harmonised C-ITS," C-Roads, [Online]. Available: https://www.c-roads.eu/fileadmin/user_upload/media/Dokumente/Harmonised_specs_text.pdf. [Accessed 4 November 2019].
[3]	ETSI, "EN 302 637-2 V1.3.2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," 2014.
[4]	ETSI, "TS 102 637-3 V1.2.2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service," 2016.
[5]	L. Gollan and C. Meinel, "Digital Signatures For Automobiles?!," *Proceedings of Systemics, Cybernetics and Informatics (SCI)*, pp. 1-5, 2002.
[6]	M. Gerlach, "Assessing and Improving Privacy in VANETs," *Proceedings of the 4th Workshop on Embedded Security in Cars (ESCAR)*, 2006.
[7]	B. Hoh, M. Gruteser, H. Xiong and A. Alrabady, "Achieving Guaranteed Anonymity in GPS Traces via Uncertainty-Aware Path Cloaking," *IEEE Transactions on Mobile Computing* , vol. 9, pp. 1089-1107, 2010.
[8]	Data Protection and Privacy Working Group of the C-ITS Platform, "Processing personal data in the context of C-ITS," 2017.
[9]	39th International Conference of Data Protection and Privacy Commissioners, "Resolution on Data Protection in Automated and Connected Vehicles," 2017.
[10]	Article 29 Data Protection Working Party, "Opinion 03/2017 on processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)," 2017.
[11]	F. Schaub, Z. Ma and F. Kargl, "Privacy Requirements in Vehicular Communication Systems," in *International Conference on Computational Science and Engineering*, 2009.
[12]	M. A. Simplicio Junior, E. Lopes Cominetti, H. Kupwade Patil, J. Ricardini, L. Ferraz and M. V. Silva, "Privacy-Preserving Method for Temporarily Linking/Revoking Pseudonym Certificates in VANETs," in *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) New York*, NY, New York, NY, 2018.
[13]	5GAA Task Force Efficient Security Provisioning, "TR E-180052 - Analysis of C-V2X security and privacy requirements and impact on SCMS design," 2018.
[14]	M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security - Special Issue on Security of Ad-hoc and Sensor Networks*, vol. 15, no. 1, pp. 39-68, 2007.
[15]	Car-2-Car Communication Consortium, "Car-2-Car Communication Consortium - FAQ regarding Data Protection in C-ITS. Number TR 2051, Version 1.0.0," 2018.
[16]	S. Lefèvre, J. Petit, R. Bajcsy, C. Laugier and F. Kargl, "Impact of V2X privacy strategies on Intersection Collision Avoidance systems," in IEEE *Vehicular Networking Conference*, 2013.
[17]	SAE Standard J2945/1_201603, "On-Board System Requirements for V2V Safety Communications," 2016.
[18]	G. Baldini, R. Giuliani and E. Cano, "An Analysis of the Privacy Threat in Vehicular Ad Hoc Networks due to Radio Frequency Fingerprinting," *Mobile Information Systems*, pp. 1-13, 2017.
[19]	J. Petit, F. Schaub, M. Feiri and F. Kargl, "Pseudonym Schemes in Vehicular Networks: A Survey," *IEEE Communications Surveys & Tutorials* , vol. 17, no. 1, pp. 228 - 255, 2015.
[20]	M. Khodaei and P. Papadimitratos, "The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems," *IEEE Vehicular Technology Magazine*, vol. 10, no. 4, pp. 63 - 69, 2015.
[21]	P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung and J.-P. Hubaux, "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100 - 109, 2008.

[22]	B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hahn and R. Goudy, "A Security Credential Management System for V2X Communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3850 - 3871, 2018.
[23]	European Commission, "Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)," 2018.
[24]	O. Henniger, A. Ruddle,, H. Seudié, B. Weyl, M. Wolf and T. Wollinger, "Securing Vehicular On-Board IT Systems: The EVITA Project," in *Proceedings of the 25th Joint VDI/VW Automotive Security Conference*, Ingolstadt, Germany, 2009.
[25]	P. Papadimitratos, . L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung and M. Raya, "Architecture for Secure and Private Vehicular Communications," in *7th International Conference on ITS Telecommunications*, Sophia Antipolis, France, 2007.
[26]	PRECIOSA, "PRivacy Enabled Capability In Cooperative Systems and Safety Applications - D1," 2009.
[27]	PRESERVE, "Security requirements of vehicle security architecture - D1.1," 2011.
[28]	5G Automotive Association; WG7 "Security and Privacy", "5GAA Efficient Security Provisioning System," 2020.
[29]	M. Wolf and T. Gendrullis, "Design, Implementation, and Evaluation of a Vehicular Hardware Security Module," in *International Conference on Information Security and Cryptology*, 2011.
[30]	Car-2-Car Communication Consortium, "Position Paper regarding personal data protection aspects in C-ITS," 2017.
[31]	ETSI, "TS 102 731 V1.1.1 - Intelligent Transport Systems (ITS); Security; Security Services and Architecture," 2010.
[32]	M. E. Nowatkowski, J. E. Wolfgang, C. McManus and H. L. Owen, "The effects of limited lifetime pseudonyms on certificate revocation list size in VANETS," in *Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)*, Concord, NC, USA, 2010.
[33]	V. Kumar, J. Petit and W. Whyte, "Binary hash tree based certificate access management for connected vehicles," in In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '17)*, New York, NY, 2017.
[34]	M. A. Simplicio, E. L. Cominetti, H. Kupwade Patil, J. E. Ricardini and M. V. M. Silva, "ACPC: Efficient revocation of pseudonym certificates using activation codes," *Ad Hoc Networks*, 2019.
[35]	USDOT, "DOT HS 812 014 - Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application," 2014.
[36]	M. A. Simplicio, E. L. Cominetti, H. Kupwade Patil, J. E. Ricardini, L. T. D. Ferraz and M. V. M. Silva, "Privacy-Preserving Certificate Linkage/Revocation in VANETs Without Linkage Authorities," *IEEE Transactions on Intelligent Transportation Systems*, 2020.
[37]	M. Moser, D. Estor, M. Minzlaff, A. Weimerskirch and L. Wolleschensky, "Operating a Car-to-X PKI - Challenges for Security and Privacy," in *FISITA 2014 World Automotive Congress*, Maastricht, Netherlands, 2014.
[38]	IETF, "RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".
[39]	B. Edelman, "Adverse selection in online «trust» certifications," in *Proceedings of the 11th International Conference on Electronic Commerce*, Taipei, Taiwan, 2009.
[40]	C. Vaas, M. Khodaei, P. Papadimitratos and I. Martinovic, "Nowhere to hide? Mix-Zones for Private Pseudonym Change using Chaff Vehicles," in IEEE Vehicular Networking Conference (VNC), Taipei, Taiwan, Taiwan, 2018.
[41]	L. Buttyán, T. Holczer, A. Weimerskirch and W. Whyte, "SLOW: A Practical pseudonym changing scheme for location privacy in VANETs," in IEEE Vehicular Networking Conference (VNC), Tokyo, Japan, 2009.
[42]	M. Khodaei, H. Noroozi and P. Papadimitratos, "Privacy Preservation through Uniformity," in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, Stockholm, Sweden, 2018.
[43]	B. Wiedersheim, Z. Ma , F. Kargl and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Seventh International Conference on Wireless On-demand Network Systems and Services (WONS)*, Kranjska Gora, Slovenia, 2010.

[44]	K. Emara, W. Woerndl and J. Schlichter, "Vehicle tracking using vehicular network beacons," in *IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, Madrid, Spain, 2013.
[45]	ETSI, "TR 103 415 - Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management," 2018.
[46]	Article 29 Data Protection Working Party, "Opinion 05/2014 on Anonymisation Techniques," 2014.
[47]	G. Neven, G. Baldini, J. Camenisch and R. Neisse, "Privacy-preserving attribute-based credentials in cooperative intelligent transport systems," in *IEEE Vehicular Networking Conference (VNC)*, Torino, Italy, 2017.
[48]	J. M. de Fuentes, L. González-Manzano, J. Serna-Olvera and F. Veseli, "Assessment of attribute-based credentials for privacy-preserving road traffic services in smart cities," *Personal and Ubiquitous Computing*, vol. 21, no. 5, p. 869–891, 2017.
[49]	J. Whitefield, L. Chen, T. Giannetsos, S. Schneider and H. Treharne, "Privacy-enhanced capabilities for VANETs using direct anonymous attestation," in *IEEE Vehicular Networking Conference (VNC)*, Torino, Italy, 2017.
[50]	T. Giannetsos and I. Krontiris, "Securing V2X Communications for the Future - Can PKI Systems offer the answer?," in *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019)*, Canterbury, United Kingdom, 2019.
[51]	ETSI, "TS 103 097 Intelligent Transport Systems (ITS); Security; Security Header and Certificate," 2017.
[52]	EU Commission, "COM(2016) 766 final - A European strategy on Cooperative Intelligent Transport Systems, a milestone towards," 2016.
[53]	M. Khodaei, H. Jin and P. Papadimitratos, "Towards deploying a scalable & robust vehicular identity and credential management infrastructure," in *IEEE Vehicular Networking Conference (VNC)*, 2014.
[54]	J. Douceur, "The Sybil Attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, 2002.
[55]	Data Protection WG of the C-ITS Platform, "Processing personal data in the context of C-ITS," 2017.
[56]	A. Tesei, L. Di Mauro, M. Falcitelli, S. Noto and P. Pagano, "IOTA-VPKI: a DLT-based and Resource Efficient," in *IEEE 88th Vehicular Technology Conference (VTC-Fall)*, Chicago, IL, USA, 2018.
[57]	"AUTOmated driving Progressed by Internet of Things (AUTOPILOT)," [Online]. Available: https://autopilot-project.eu/. [Accessed 5 November 2019].
[58]	NGMN Alliance, "V2X White Paper," 2018.

5GAA is a multi-industry association to develop, test and promote communications solutions, initiate their standardisation and accelerate their commercial availability and global market penetration to address societal need. For more information such as a complete mission statement and a list of members please see https://5gaa.org


5GAA
Automotive Association