5GAA
Automotive Association

V2N2X security, privacy, and data quality

5G Automotive Association
Position Paper

CONTACT INFORMATION:
Executive Manager – 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:	20 December 2024
DOCUMENT TYPE:	Position Paper
EXTERNAL PUBLICATION:	Yes
DATE OF APPROVAL BY 5GAA BOARD:	21 November 2024

Introduction

Cellular Vehicle-to-Everything (C-V2X) is an umbrella term that encompasses all 3GPP V2X technologies, including both direct (PC5) and mobile network communications (Uu). In many cases, both direct and network modes of C-V2X can be used for the same or similar automotive and Intelligent Transport System (ITS) applications, yet with different service characteristics. However, there are fundamental differences when it comes to the architecture and realisation of different Use Cases (UC) applying mobile network vs. direct (short-range) communications. This leads to different ways of handling security, privacy, and how to ensure data quality – the fundamental requirements of every ITS service – when using C-V2X mobile network communication or direct communication. This is already reflected in other organisations such as ITS America[1].

This 5GAA paper provides an overview on how security, privacy, and data quality are addressed for C-V2X using mobile network and backend communications, also known as Vehicle-to-Network-to-Everything (V2N2X) solutions.

1. System architecture and ecosystem overview

To understand how security, privacy, and data quality are addressed for a V2N2X solution, it is helpful to look at 5GAA's applied V2N2X application reference architecture[2] (Figure 1).

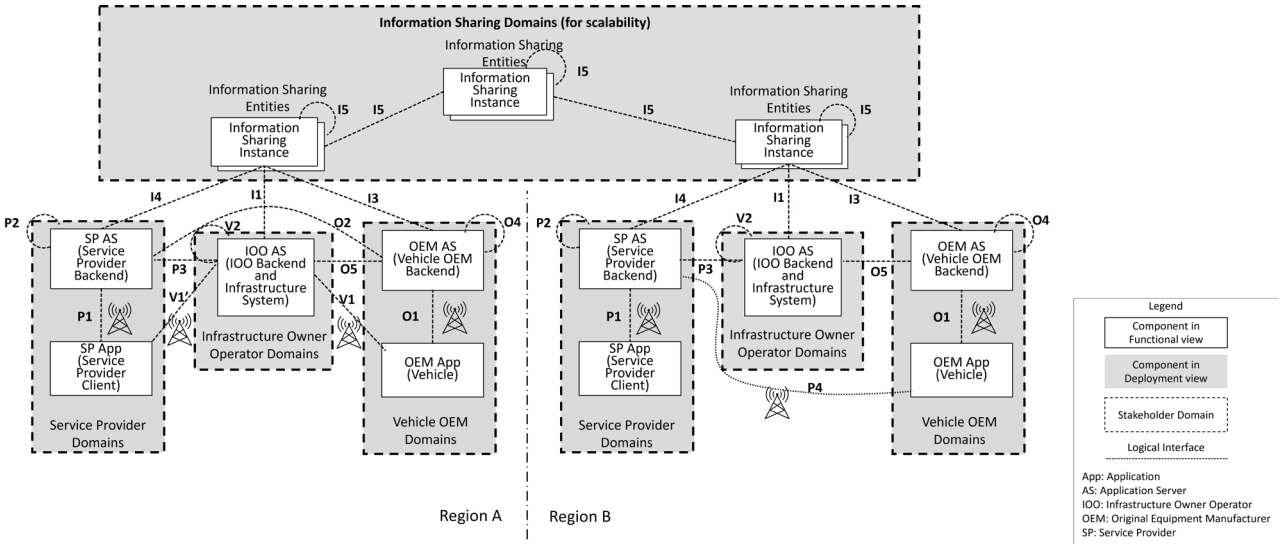

Figure 1 Applied application reference architecture (Source: 5GAA)

1 https://itsa.org/wp-content/uploads/2024/08/ITSA-B5.9-2024-Deployment-Plan_FINAL-PDF.pdf

2 https://5gaa.org/road-traffic-operation-in-a-digital-age-a-holistic-cross-stakeholder-approach

Stakeholder domains for Service Providers (SPs), Infrastructure Owner Operators (IOOs), and vehicle OEMs are lined up at the bottom of Figure 1. Stakeholders are fully responsible for services and implementation of interfaces within their own domains. Illustrating setups from two regions, multiple instances of SP/IOO/OEM domains are connected to different Information Sharing Instances (ISI) to create an interconnected V2N2X ecosystem. In addition, stakeholders may be bidirectionally connected. The Information Sharing Domain on top of the stakeholder domains is designed to enable data sharing among the stakeholders. Within the Information Sharing Domain multiple interconnected ISIs can form a decentralised system. An ISI may, for example, be responsible for a state, region, or country. The Information Sharing Domain can also provide data federation, through which one connected stakeholder domain can obtain information published by another connected stakeholder domain.

In addition to system components and interfaces shown in Figure 1, additional measures and functions are needed for a V2N2X system to operate ITS services across multiple ecosystem stakeholders. Such functions include 'governance', 'ecosystem initialisation', as well as other key functions in the run-time operation for ITS services.

- 'Governance' is an important part of a V2N2X solution involving multiple ecosystem stakeholders. The governance includes defining a Common Code of Conduct (CCoC) for data sharing, data quality, and the security and privacy of end users. Governance components also oversee the CCoC, and ensure that an agreed framework is adhered to by interconnected stakeholders – some of which can be handled through bilateral agreements.
- 'Ecosystem initialisation' comprises the discovery of services and actors, distribution of credentials to trusted actors. Again, for a limited number of such actors, this can be handled bilaterally.
- Key functions during the run-time of a V2N2X solution include monitoring data quality and system operation and providing a federated information sharing network.

In addition to the different handling of security, privacy, and data quality compared to direct short-range communications, V2N2X solutions can also be interoperable at the application- and service- levels rather than at the radio level[3]. Geo-referencing, in combination with standard IP and message queuing protocols, are used in a V2N2X solution to address and deliver information to ITS stations in a specific area. Further details about the architecture, functional differences and how to realise UCs for a V2N2X solution are described in earlier 5GAA documents[4].

2. Security

2.1. Security within a stakeholder domain

Within their own stakeholder domain, SPs, IOOs, or OEMs are fully responsible for their services and need to maintain security, privacy, data quality, etc. The Application

3 Application Servers provide the bridge between users on different mobile networks, allowing different radio-specific parts of the protocols being used in different networks. An AS can then provide service-level interoperability, i.e., pass the application-level information on to other actors, and if necessary, convert the application-level information to an agreed format before passing it on.

4 https://5gaa.org/vehicle-to-network-to-everything-v2n2x-communications-architecture-solution-blueprint-use-cases/

Server (AS), i.e., the backend system, and the 'App' is operating according to a standard client-server concept over cellular networks (O1 and P1 interfaces in Figure 1). This means that security solutions, including authentication, encryption, etc., specified in 3GPP standards are applied. Since this communication between AS and App is crucial for ITS service operation and business, the communication on these internal interfaces (O1, P1) are also protected on the application layer and/or transport- and network layer using state-of-the-art technology, such as Transport Layer Security (TLS). The implementation details of the security solution in a stakeholder domain are decided by the domain owner.

2.2. Security between stakeholder domains

Figure 1 shows a number of interfaces between stakeholder domains, i.e. P2, V2, O4, O2, O5, P3, P4, V1. These interfaces may be based on bilateral agreement between stakeholders and thus trust is based on contractual agreements. Figure 1 also show a number of interfaces between stakeholder domains and Information Sharing Domain, i.e. I1, I3, I4, and I5 the interface between the Information Sharing Instances (ISIs). Such interfaces are used when an ecosystem for information sharing is established. Participants need to agree on the CCoC, related contractual conditions, and pass related authentication and verification steps before joining the ecosystem as a trusted stakeholder.

If an App (client) in one stakeholder domain should communicate with an AS in another stakeholder domain, this is always controlled by the App's backend system/server. For example , an OEM backend could allow an OEM App in a vehicle to establish a connection to an SP AS. In such cases an agreement has been established between the stakeholders. Security credentials, address information of the AS, etc. have to be exchanged between the backend systems prior to the established connection. Examples of such a setup are Automated Valet Parking and Automated Vehicle Marshalling[5] [6].

Technically, these communication interfaces are using standard IP technology and security methods, such as TLS with standard X509 certificates and mutual authentication, and they operate in a client-server fashion. The key aspect in this relationship is that everyone involved knows the other party it is communicating with, i.e., knows the responsible entity/entities if security or data quality is compromised. When ISIs are used, additional functions monitor behaviour and data quality (further elaborated in the 'Data quality' section).

2.3. Credential handling for security domains

The AS entities used for communicating with other stakeholders are separate from the stakeholder internal domain and therefore use different certificates for related communications, keeping the internal security domain isolated from the external security domain.

In the initial stages/rollout of the solution – or indeed if only a limited number of stakeholders establish backend communication links for information sharing – bilateral

5 https://5gaa.org/content/uploads/2023/09/5gaa-wi-avp.pdf

6 https://www.vda.de/en/news/publications/publication/automated-valet-parking-systems

agreements may be used and security credentials (e.g., X509 certificates) can be provided by either party. However, as the ecosystem of interconnected actors in a V2N2X solution scale up and begin to use ISIs, then it is reasonable and helpful to employ one or a few common Root Certificate Authorities (CAs) to create common trust anchor(s) for backend communications, i.e., leverage standard IT technology and CAs and create a trust domain with a dedicated PKI for the ecosystem. Common trust anchor(s) can help to align efforts, avoiding individual solutions on each connection, thus allowing greater flexibility, e.g., redirecting stakeholder connections to other actors using the same trust anchor, which in turn optimises the data path to a data source. Redirects like this could prove useful when large amounts of data are involved or more time critical data needs to be transferred, such as Signal Phase and Timing (SPaT) data.

Furthermore, for scalability and operational reasons, intermediate CAs could be used to issue and distribute the X509 certificates to the approved actors. Depending on the trust model agreed, the X509 certificates could be used for signing shared information to help trace the originator. Alternatively trust may instead be based on agreements among actors, complemented by technical measures such as adding an actor identifier to the shared information, applying validation steps for shared information and logging, and other approaches to further ensure traceability.

2.4. Interaction between different security domains

If a stakeholder is a trusted actor in the V2N2X domain[7], and if the stakeholder is also enrolled in the Direct Communication (DC) domain, adhering to the rules applying to that domain, the stakeholder can act as a bridge between the domains. This means stakeholders receiving a message via DC can verify the quality and take responsibility for the information before sharing it with other interconnected backend systems, or via the Information Sharing Domain. If stakeholders obtain information from interconnected backend systems or the Information Sharing Domain and intend to forward it with DC, the stakeholder can create a message according to the standard used in the DC domain.

3. Privacy

Privacy should be governed by contracts through the agreed CCoC and complemented by technical measures. **For communication within a stakeholder domain**, e.g., between an SP AS and the SP App or between an OEM AS and the OEM App, privacy is protected subject to the decision of the respective party – e.g., using TLS connections for integrity and confidentiality to prevent the leakage of sensitive private information.

In this case, user consent for the AS on whether and how to handle personal data needs to be in place as part of the acceptance procedure granting access to the services.

7 Stakeholder adhering to a Common Code of Conduct signs and respects the contractual terms regarding data quality, security, validation, etc.

For communication with and in the Information Sharing Domain, secured connections (e.g., based on TLS) are used for I1, I3, I4, I5 interfaces between authorised and trusted actors, see Figure 1, to ensure the integrity and confidentiality of the communication. Additionally, for the actual information (payload data) conveyed, before an AS transmits anything through the Information Sharing Domain, it should ensure that the data does not contain personal details (e.g., by applying data anonymisation methods). This means if the payload contains personal data – i.e., based on received information from an SP App or OEM App – the AS should remove any private information before transmitting it.

If identity information is required by the V2X UC, the AS may use an own identifier within the anonymised data-set, e.g., insert a default identifier for the AS. In many cases, an AS improves payload data quality by analysing and fusing multiple inputs from individual SP Apps or OEM Apps. In such cases, it would be normal and common practice for the AS to use the default identifier to transmit the processed data instead of individual identification of the SP Apps or OEM Apps.

For V2X Use Cases requiring two-way communication (e.g., requesting traffic signal priority and receiving a response) in order to protect the privacy of the requester, the requesting AS can act as a proxy – allocating temporary identifiers and using them in the request message. When receiving a response, the AS can map back to the actual requester, thus protecting their personal data.

4. Data quality

Agreements, contracts, and various governance measures feed an ecosystem of rules and tools for ensuring data quality, i.e. an actor providing data to a business partner or other entity in the ecosystem has to commit to a data quality regime. As the communicating actors are known to each other, the source of faulty or bad data can be clearly identified. Functions should also be in place to support the validation and logging of shared information in order to facilitate traceability, analyse whether bilateral quality criteria are being fulfilled, identify misbehaving/malfunctioning components or systems, and monitor adherence with the established CCoC and corresponding quality agreements. One method to ensure data quality is for the AS to evaluate information from different 'Apps' (clients) before sharing data with the ecosystem (or to a business partner).

A common conceptual tool in decision-making is the Plan-Do-Check-Act (PDCA) cycle. Its four stages help planners avoid recurring mistakes, and it is a feature of lean manufacturing and project management. The order of the model or cycle has been rearranged slightly in the context of V2N2X, as shown in Figure 2:

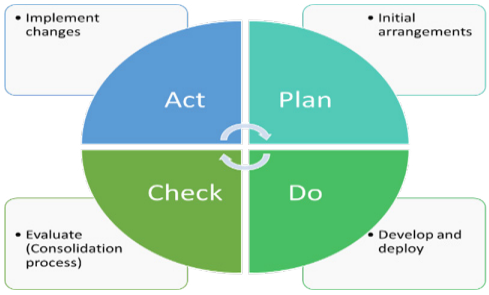

Figure 2 PDCA applied to the V2N2X scenario (Source: 5GAA)

Large-scale deployments require consistent, well-structured data quality control and corrective countermeasures in order to deliver services to the many different road users[8]. As illustrated in the above PDCA model, quality management is a continuous process that starts with an initial agreement on the (quality) standards, which is usually part of the ecosystem's CCoC. Quality elements in the CCoC range from selfassessments to product- and organisation certifications, online monitoring, and automatic sanity checks.

With the quality elements properly described (in the CCoC), access to the Information Sharing Domain is restricted to parties and products that meet requirement as described in the CCoC. This should be governed by the organisation that manages a particular Information Sharing Instance or through a neutral governing body. Examples of suitable governing bodies are already abundantly present in the transport ecosystem.

To ensure the highest overall quality, continuous data quality control and enforcement is needed on top of the initial agreements or arrangements. The networked V2X path offers ideal opportunities for this due to the presence of the ISIs, playing a central role in automated quality monitoring, such as:

- Monitoring connection quality (uptime, latency, etc.);
- Monitoring message quality (conformity, 'odd' values, pattern analysis, etc.);
- Monitoring the trustworthiness of the data path itself, essentially assessing the security and reliability of the data path and various nodes that data passes through;
- Monitoring UC quality (e.g., usage and impact).

This continuous and automated monitoring takes quality control to the next level – i.e., automated enforcement of quality. ISIs can use policy agreements to set clear expectations for data quality. These agreements define acceptable ranges for metrics like latency, integrity, and trustworthiness. ISIs can dynamically enforce these standards across multiple domains. When a source fails to meet required quality or trust levels, this could trigger a set of escalating (re)actions depending on the nature of the quality breach - ranging from flagging and quarantining messages to blocking connections from certain actors. Again, the ISIs are ideally situated to perform the automated enforcement of quality.

Combined, this set of measures and actions leads to more reliable and consistent (data) quality paving the way for large-scale deployment and the benefits that accrue from that for the widest range of road users today and in the future.

The 5G Automotive Association (5GAA) is a global, cross-industry organisation of over 115 members, including leading global automakers, Tier-1 suppliers, mobile operators, semiconductor companies, and test equipment vendors. 5GAA members work together to develop end-to-end solutions for future mobility and transport services. 5GAA is committed to helping define and develop the next generation of connected mobility, automated vehicles, and intelligent transport solutions based on C-V2X.

For more information, please visit https://5gaa.org


5GAA
Automotive Association