International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1372

(03/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Intelligent transportation system (ITS) security

# Security guidelines for vehicle-to-everything (V2X) communication

Recommendation ITU-T X.1372

ITU-T X-SERIES RECOMMENDATIONS

**DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY**

| | |
|---|---|
| PUBLIC DATA NETWORKS | X.1–X.199 |
| OPEN SYSTEMS INTERCONNECTION | X.200–X.299 |
| INTERWORKING BETWEEN NETWORKS | X.300–X.399 |
| MESSAGE HANDLING SYSTEMS | X.400–X.499 |
| DIRECTORY | X.500–X.599 |
| OSI NETWORKING AND SYSTEM ASPECTS | X.600–X.699 |
| OSI MANAGEMENT | X.700–X.799 |
| SECURITY | X.800–X.849 |
| OSI APPLICATIONS | X.850–X.899 |
| OPEN DISTRIBUTED PROCESSING | X.900–X.999 |
| INFORMATION AND NETWORK SECURITY | |
| General security aspects | X.1000–X.1029 |
| Network security | X.1030–X.1049 |
| Security management | X.1050–X.1069 |
| Telebiometrics | X.1080–X.1099 |
| SECURE APPLICATIONS AND SERVICES (1) | |
| Multicast security | X.1100–X.1109 |
| Home network security | X.1110–X.1119 |
| Mobile security | X.1120–X.1139 |
| Web security | X.1140–X.1149 |
| Security protocols (1) | X.1150–X.1159 |
| Peer-to-peer security | X.1160–X.1169 |
| Networked ID security | X.1170–X.1179 |
| IPTV security | X.1180–X.1199 |
| CYBERSPACE SECURITY | |
| Cybersecurity | X.1200–X.1229 |
| Countering spam | X.1230–X.1249 |
| Identity management | X.1250–X.1279 |
| SECURE APPLICATIONS AND SERVICES (2) | |
| Emergency communications | X.1300–X.1309 |
| Ubiquitous sensor network security | X.1310–X.1319 |
| Smart grid security | X.1330–X.1339 |
| Certified mail | X.1340–X.1349 |
| Internet of things (IoT) security | X.1360–X.1369 |
| **Intelligent transportation system (ITS) security** | **X.1370–X.1389** |
| Distributed ledger technology security | X.1400–X.1429 |
| Distributed ledger technology security | X.1430–X.1449 |
| Security protocols (2) | X.1450–X.1459 |
| CYBERSECURITY INFORMATION EXCHANGE | |
| Overview of cybersecurity | X.1500–X.1519 |
| Vulnerability/state exchange | X.1520–X.1539 |
| Event/incident/heuristics exchange | X.1540–X.1549 |
| Exchange of policies | X.1550–X.1559 |
| Heuristics and information request | X.1560–X.1569 |
| Identification and discovery | X.1570–X.1579 |
| Assured exchange | X.1580–X.1589 |
| CLOUD COMPUTING SECURITY | |
| Overview of cloud computing security | X.1600–X.1601 |
| Cloud computing security design | X.1602–X.1639 |
| Cloud computing security best practices and guidelines | X.1640–X.1659 |
| Cloud computing security implementation | X.1660–X.1679 |
| Other cloud computing security | X.1680–X.1699 |
| QUANTUM COMMUNICATION | |
| Terminologies | X.1700–X.1701 |
| Quantum random number generator | X.1702–X.1709 |
| Framework of QKDN security | X.1710–X.1711 |
| Security design for QKDN | X.1712–X.1719 |
| Security techniques for QKDN | X.1720–X.1729 |
| DATA SECURITY | |
| Big Data Security | X.1750–X.1759 |
| 5G SECURITY | X.1800–X.1819 |

*For further details, please refer to the list of ITU-T Recommendations.*

# Recommendation ITU-T X.1372

## Security guidelines for vehicle-to-everything (V2X) communication


### Summary

Recommendation ITU-T X.1372 provides security guidelines for vehicle-to-everything (V2X) communication. V2X is a generic term for the communication modes termed as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-nomadic devices (V2D) and vehicle-to-pedestrian (V2P) discussed in this Recommendation.

Significant developments have taken place over the past few years in the area of vehicular communication in the intelligent transportation system (ITS) environment. The V2X communication significantly improves road safety, decreases traffic congestion and increases convenience. However, V2X communication also makes relevant entities in the ITS environment vulnerable to various forms of cyber-attack.

To address this security problem, this Recommendation identifies threats in V2X communication environments and specifies security requirements for V2X communication to mitigate these threats. This Recommendation also provides description of possible implementation of V2X communication with security.



### History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1372 | 2020-03-26 | 17 | 11.1002/1000/14091 |

### Keywords

ITS security, risk analysis, security requirements, threat analysis, V2I, V2V, V2D, V2P, V2X.


* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

## Table of Contents

# Recommendation ITU-T X.1372

## Security guidelines for vehicle-to-everything (V2X) communication

### 1 Scope

This Recommendation provides security guidelines for vehicle-to-everything (V2X) communication. V2X is a generic term comprising the communication modes termed as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-nomadic devices (V2D) and vehicle-to-pedestrian (V2P) when discussed in this Recommendation. This Recommendation identifies threats in the V2X communication environment, specifies security requirements and provides description of possible implementation of V2X communication with security.

Specific security controls for V2X communication are out of scope of this Recommendation.

### 2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 accountability** [b-ITU-T X.800]: The property that ensures that the actions of an entity may be traced uniquely to the entity.

**3.1.2 authenticity** [b-ITU-T X.641]: Protection for mutual authentication and data origin authentication.

**3.1.3 authentication** [b-ITU-T X.1252]: A process used to achieve sufficient confidence in the binding between the entity and the presented identity.

NOTE – Use of the term authentication in an identity management (IdM) context is taken to mean entity authentication.

**3.1.4 authorization** [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

**3.1.5 availability** [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

**3.1.6 certification authority (CA)** [b-ITU-T X.509]: An authority trusted by one or more entities to create and digital sign public-key certificates. Optionally the certification authority may create the subjects' keys.

**3.1.7 confidentiality** [b-ITU-T X.800]: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

**3.1.8 integrity** [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

**3.1.9 message authentication code (MAC)** [b-ITU-T X.813]: A cryptographic checkvalue that is used to provide data origin authentication and data integrity.

**3.1.10 nomadic devices** [b-ITU-T F.749.1]: Nomadic devices include all types of information and communication devices as well as entertainment devices that can be brought into the vehicle by the driver and/or passengers to be used while driving. Examples include mobile phones, portable computers, tablets, mobile navigation devices, portable media players and multi-functional smart phones.

**3.1.11 non-repudiation with proof of origin** [b-ITU-T X.800]: The recipient of data is provided with proof of the origin of data. This will protect against any attempt by the sender to falsely deny sending the data or its contents.

**3.1.12 pseudonym** [b-ITU-T X.1252]: An identifier whose binding to an entity is not known or is known to only a limited extent, within the context in which it is used.

NOTE – A pseudonym can be used to avoid or reduce privacy risks associated with the use of identifier bindings which may reveal the identity of the entity.

**3.1.13 public-key certificate (PKC)** [b-ITU-T X.509]: The public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority (CA) that issued it.

## 3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

**3.2.1 misbehaviour**: Behaviour that results in devices sending wrong information that could cause other devices to take incorrect actions; or devices taking the wrong action despite receiving the correct information.

# 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|---|---|
| AES | Advanced Encryption Standard |
| AVN | Audio, Video, and Navigation |
| CA | Certification Authority |
| CAMP | Crash Avoidance Metrics Partnership |
| CCM | Counter mode with cipher block chaining message authentication code |
| CCU | Central Communication Unit |
| DDoS | Distributed Denial of Service |
| EEBL | Electronic Emergency Brake Light |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| ECIES | Elliptic Curve Integrated Encryption Scheme |
| ECU | Electronic Control Unit |
| GPS | Global Positioning System |
| HDMI | High-Definition Multimedia Interface |
| ID | Identifier |

| | |
|---|---|
| ITS | Intelligent Transportation System |
| IVN | In-Vehicle Network |
| KDF | Key Derivation Function |
| LDM | Local Dynamic Map |
| LOS | Line Of Sight |
| LTE | Long Term Evolution |
| MAC | Message Authentication Code |
| MHL | Mobile High-definition Link |
| NFC | Near Field Communication |
| NGN | Next Generation Networks |
| NLOS | Non-Line Of Sight |
| OBD | On Board Diagnostics |
| OBU | On-Board Unit |
| PII | Personally Identifiable Information |
| PKI | Public-Key Infrastructure |
| QoS | Quality of Service |
| RSU | Road-Side Unit |
| SCMS | Security Credential Management System |
| SHA | Secure Hash Algorithm |
| USB | Universal Serial Bus |
| V2I | Vehicle-to-Infrastructure |
| V2D | Vehicle-to-nomadic Device |
| V2P | Vehicle-to-Pedestrian |
| V2V | Vehicle-to-Vehicle |
| V2X | Vehicle-to-everything |
| VGP | Vehicle Gateway Platform |
| VRU | Vulnerable Road User |
| WAVE | Wireless Access in Vehicular Environments |
| WiFi | Wireless Fidelity |

## 5 Conventions

None

## 6 V2X communication

### 6.1 Overview

Intelligent transportation systems (ITS) include a broad range of information and communication technologies that are designed to improve safety and efficiency of transportation system. Significant

development has taken place over the past few years, particularly regarding vehicular communication systems.

Vehicular communication systems support the exchange of data among vehicles, between vehicles and infrastructure, and between vehicles and nomadic devices. The types of data include things like current position, vehicle speed and warnings derived from on-board sensors. In addition, road-side units (RSUs) can provide communication links to a traffic monitoring systems that collects and distribute warnings about hazardous situations among surrounding vehicles. Without security protections however, ITS can become dangerous for traffic safety as well as to human life. Therefore, security of ITS is being investigated in order to safely and successfully deploy ITS.

Figure 1 shows an overview of vehicular communication. Vehicular communication can be classified into communications external and internal to a vehicle. The internal network of a vehicle, known as the in-vehicle network (IVN), involves vehicle components such as sensors and electronic control units (ECUs). The external communications can be categorized into V2V, V2I, V2D and V2P communications. On-board units (OBUs) are the wireless communication units equipped on vehicles, whereas RSUs are wireless access units located at on the road. The infrastructure consists of RSUs and back-end facilities, such as traffic management, monitoring systems, certification authority (CA). The RSUs can be connected to the backend facilities via wired or wireless networks.

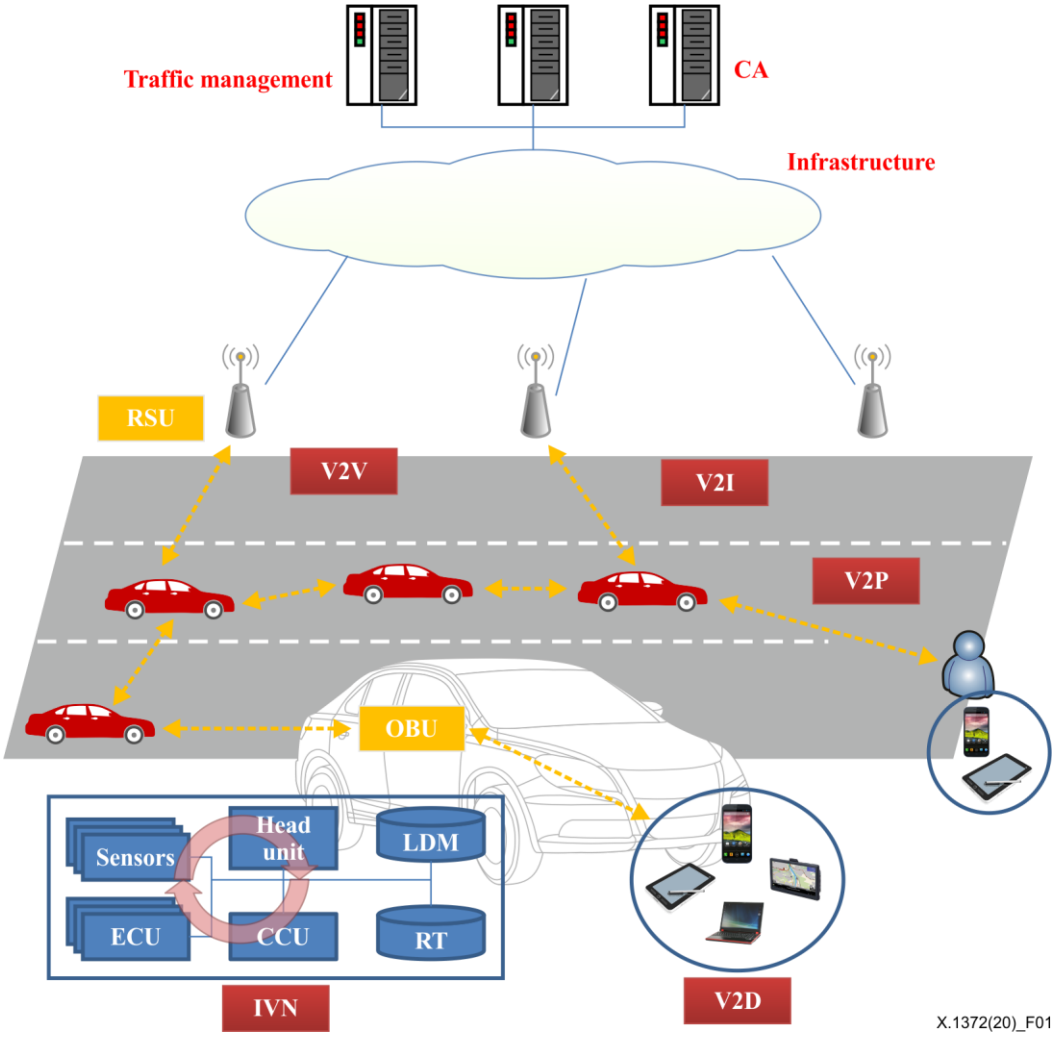



**Figure 1 – Overview of vehicular communication**

## 6.2 V2V communication

V2V communication includes the wireless transmission of data among vehicles. The purpose of V2V communication is to prevent accidents by sharing and sending information among vehicles. Depending on how V2V technology is implemented, a vehicle may receive a warning that informs it of a possible risk of an accident. The vehicle may then take pre-emptive actions such as braking to slow down. Platoon communication in V2V could make group driving possible by sharing speed and road conditions. Additionally, beaconing could be used for information exchange among vehicles to support easy and safe driving. With the support of V2V communication, a vehicle can gather information that includes 360-degree awareness of its surrounding environments.

The following V2V communication scenarios can be identified.

– V2V warning propagation:

  In a V2V warning propagation scenario, a warning message is propagated from one vehicle to another. For example, if there is a traffic accident, a warning should be transmitted backward to all vehicles approaching the accident, informing them that there has been a collision ahead. On the other hand, if an emergency vehicle such as a police car is approaching from behind, a warning message should be transmitted forward to all vehicles nearby and ahead so that an emergency vehicle may safely approach at high speed. Figure 2 illustrates a situation in which a forward accident warning propagates rearward and Figure 3 illustrates a situation in which the emergency vehicle coming from behind and the warning message propagates forward;

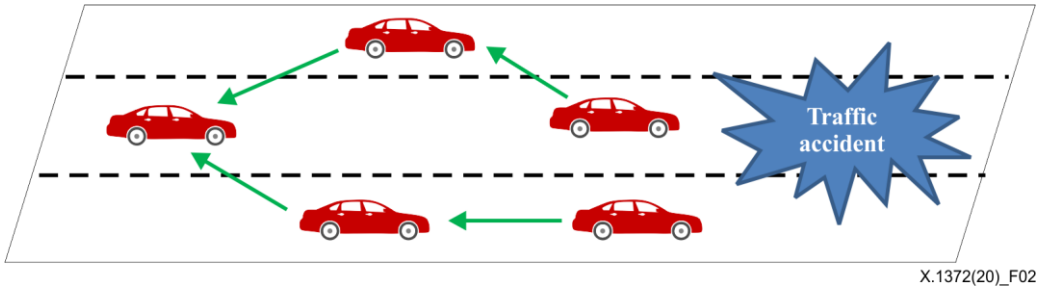



**Figure 2 – V2V warning propagation – rearward propagation**

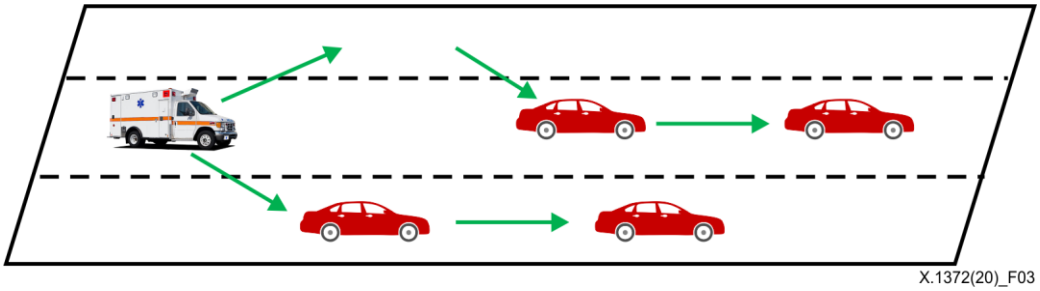



**Figure 3 – V2V warning propagation – forward propagation**

– V2V platoon communication:

  In a V2V platoon communication scenario, several vehicles form a group that can communicate with each other within this group. For example, vehicles taking the same route, or at least the same route for some time, can form a platoon. This group can communicate vehicle status information to assist with safe driving. Figure 4 illustrates V2V platoon communication;

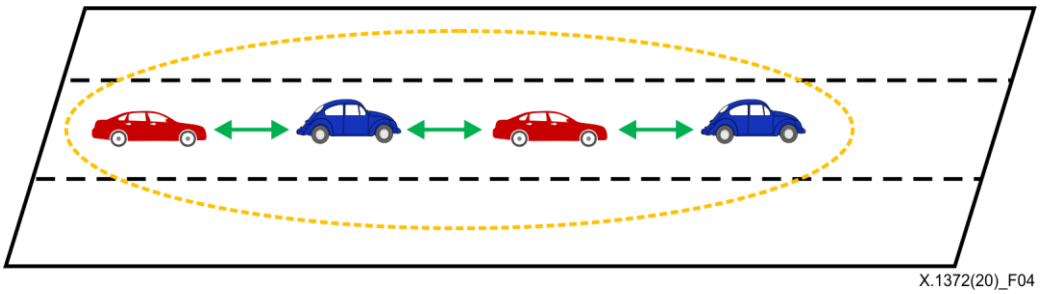



**Figure 4 – V2V platoon communication**

– V2V beaconing:

In a V2V beaconing scenario, each vehicle periodically sends its vehicle status information, such as current speed, heading and position to nearby vehicles. Figure 5 illustrates V2V beaconing.

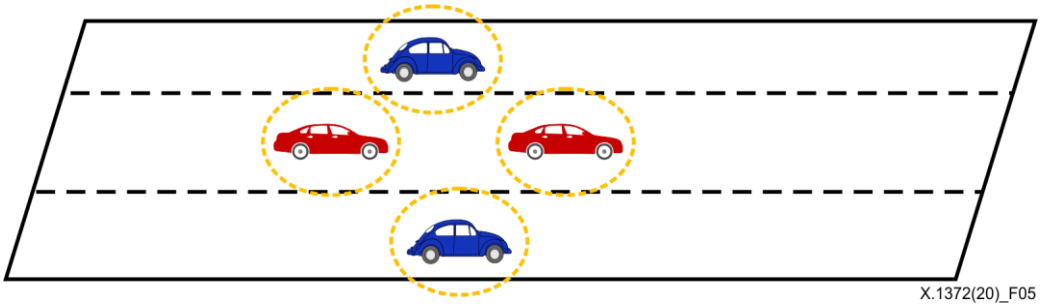



**Figure 5 – V2V beaconing**

### 6.3 V2I communication

Vehicle-to-infrastructure (V2I) communication is the wireless transmission of data between a vehicle and infrastructure such as a road-side unit (RSU).

The following V2I communication scenarios can be identified.

– V2I warning:

V2I warning scenario allows communication between a vehicle and infrastructure, such as RSUs. For example, when a traffic accident occurs at an intersection, an RSU could send a warning message to vehicles that are approaching the intersection. Alert notifications of vehicle proximity in the case of lane entry negotiation at the right or left-turning and confluent points are also V2I warning use cases. Figure 6 shows an example V2I warning scenario;

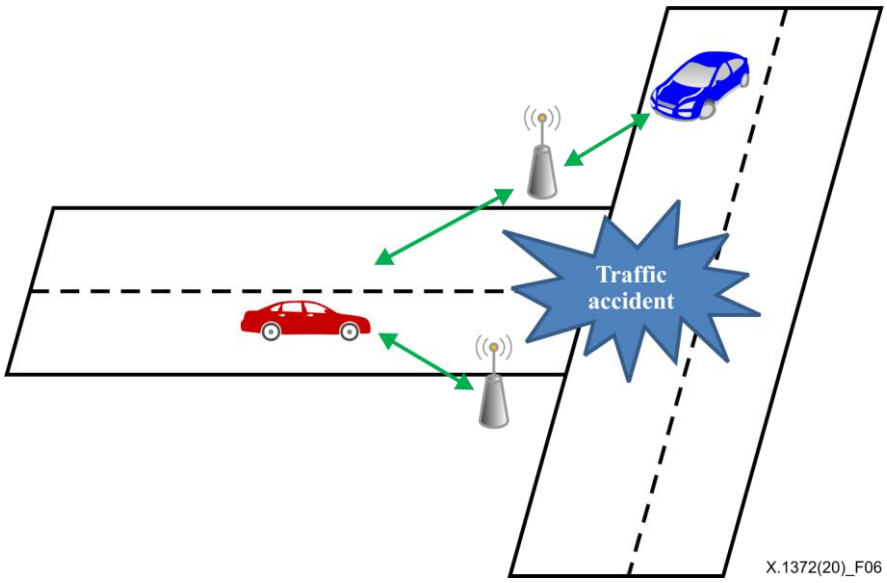



**Figure 6 – V2I warning**

– V2I information exchange (including V2V):

V2I information exchange may include information such as in-vehicle signage/information, signal phase and time of traffic light information, probe vehicle data, accounting information (e.g., toll collection), road-surface/weather/visible-distance conditions and road construction information. Examples of use cases include:

- downloading basic transport data:

  In ITS, a number of V2I messages may contain warning messages. To deal with such messages, a vehicle often requires a map of where it is located or where it is moving to, or may need real-time circumstance information surrounding the vehicle. Such information is often downloaded from infrastructure such as RSUs;

- data supporting transport efficiency:

  In ITS, a vehicle can communicate with the infrastructure occasionally in order to obtain traffic related information such as temporary traffic control information, etc. As a result, a vehicle can know where traffic jams are happening. It can then optimize its route with help from the infrastructure, e.g., by updating its route through a navigator which has mobile network connectivity. Therefore, the efficiency of vehicles can be improved using V2I communication. In another example, the infrastructure can also update traffic information based on the message provided by the vehicle through V2I communication. Figure 7 shows the V2I information exchange.

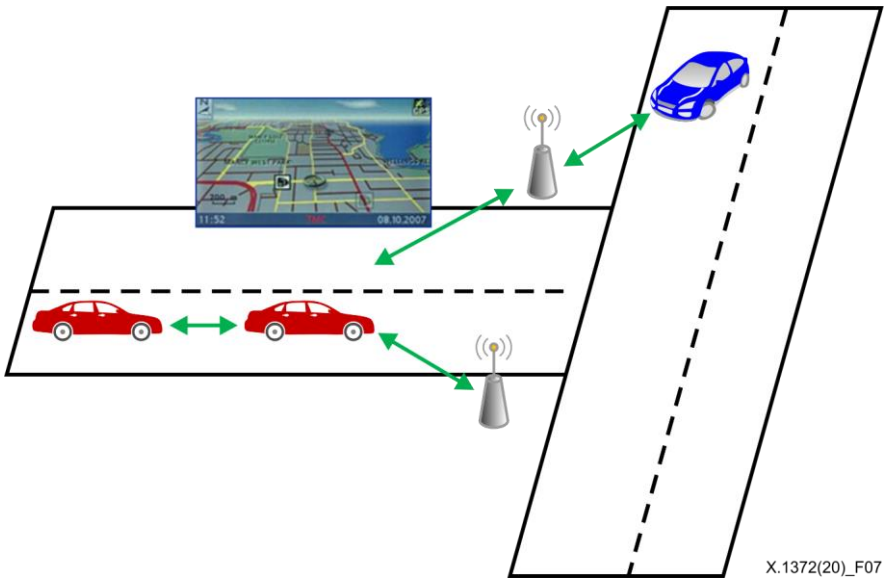



**Figure 7 – V2I information exchange**

## 6.4 V2D communication

Using V2D communication technology, a vehicle is connected to mobile devices such as smartphones, laptops and navigation systems in the vehicle, either through an open architecture with a standardized interface to the controller area network (CAN) bus of the vehicle, or by implementation of a gateway that intermediates the requests/responses from the nomadic device to the system running on the vehicle. Using a smartphone or mobile device, functions can be provided remotely to identify and manage vehicle status information such as maintenance parts. In addition, further development of convenient services is expected.

Taking for example travel planning where a driver chooses a destination on a nomadic device, the nomadic device can then plan a route by assembling different items of information from different sources such as timetables for public transportation (train, metro, buses, etc.) as well as real-time traffic information. The vehicle follows the planned route, making a detour if short-term changes in the traffic situation occur. The nomadic device not only makes decisions about manoeuvres and executes them, but also reacts to local traffic situations, e.g., following other vehicles, avoiding obstacles, changing lanes, stopping at traffic lights, etc. The nomadic device can be connected to in-vehicle networks. Therefore, attackers may possibly gain access to a vehicle's internal systems. In the case of security threats via Bluetooth, malicious code can be executed through applications on smartphones connected to the vehicle. In-vehicle audio, video, and navigation (AVN) systems are vulnerable to firmware attacks via multimedia storages and can easily be exposed to hacking via global positioning system (GPS) or satellite radio channels. Attacks through nomadic devices should be controlled to prevent risks to vehicle safety.

Discussions about two different types of V2D communication follow.

– V2D communication by indirect links:

  Vehicles and nomadic devices can communicate through indirect links. Communication by indirect links means that third-party equipment such as access points and routers provide communication between end nodes. Cellular phones and smartphones use mobile wireless broadband technology such as long-term evolution (LTE) and wireless fidelity (Wi-Fi), etc. The use of Wi-Fi in smartphones in order to communicate with vehicles is increasing. 5G technologies are also a key communication channel for these indirect links.

– V2D communication by direct links:

Vehicles and nomadic devices can communicate by direct links without any intervention between them or via wireless communication technologies such as Bluetooth, ZigBee and near field communication (NFC).

Vehicles and nomadic devices can also communicate by wired links. For example, a nomadic device can connect to a vehicle through physical access such as universal serial bus (USB), mobile high-definition link (MHL) and high-definition multimedia interface (HDMI). The on-board diagnostics II (OBD-II) standard specifies diagnostic interfaces and also provides a candidate list of vehicle parameters and procedures for transmission of the data.

In particular, V2P communication could be considered as a specific case of V2D communication when the vehicle communicates with a nomadic device associated with a pedestrian.

The V2P approach has applications for a broad set of vulnerable road users (VRUs) including non-motorized road users, such as pedestrians and cyclists as well as motorcyclists and persons with disabilities or reduced mobility.

Due to high level of traffic accidents involving VRUs, ITS proposes solutions to enhance road safety through sensor data collection and concepts such as perception and enabling of information exchange between vehicles and pedestrians. More importantly, V2P communication will not only warn a vehicle driver about an approaching pedestrian to stop the vehicle but will also alert the pedestrian's mobile phone to notify the pedestrian that the vehicle is approaching.

ITS can detect VRUs and help to prevent potential collisions between vehicles and VRUs. Figures 8 showing a pedestrian in a driver line of sight (LOS) scenario and Figure 9 showing a pedestrian in a driver non-line of sight (NLOS) scenario, serve to demonstrate how ITS can improve VRU road safety.

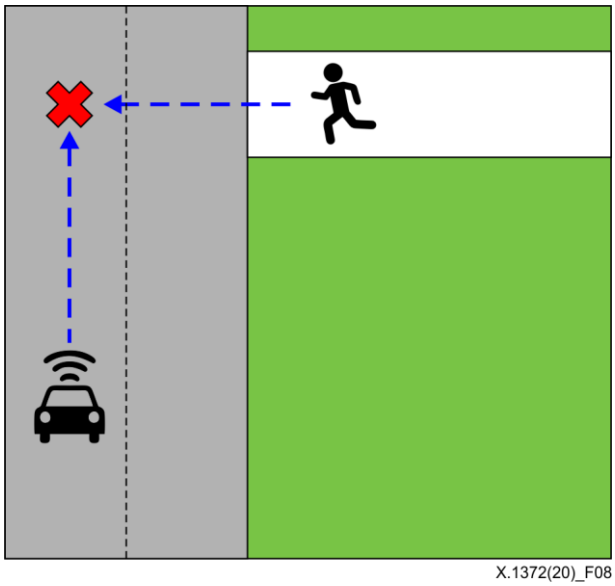



**Figure 8 – LOS**

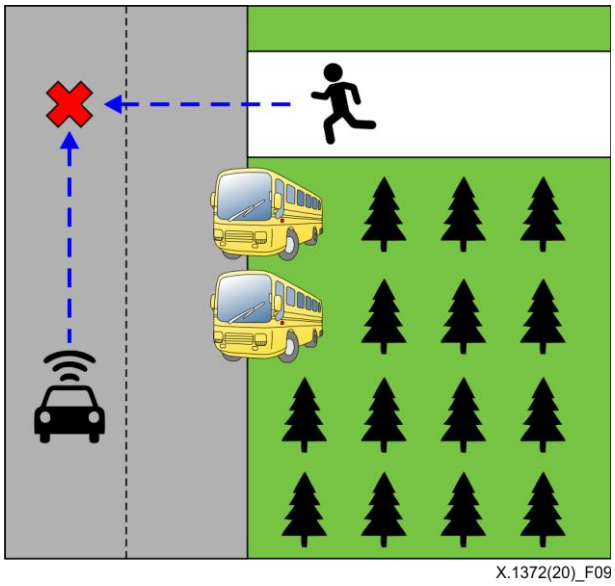



**Figure 9 – NLOS**

• pedestrian in driver LOS:

As shown in Figure 8, active sensors such as radars, ultrasonic sensors, laser rangefinders and video cameras adopt computer-vision-based methods applicable to pedestrian detection where pedestrians are visible from the vehicle. When a pedestrian is approaching, the moving vehicle will detect the pedestrian and can then make the

critical decision. At the same time, the vehicle can warn the pedestrian's cell phone to alert him of the potential danger;

- pedestrian in driver NLOS:

  The ability to detect pedestrians is limited by the sensors' field of view. In Figure 9, the pedestrian is blocked from the view by obstacles, such as trees and parking buses. Vehicular communication, however, is able to announce and disseminate information beyond the sensors' field of view. Once the vehicle has received the warning notification, it updates its local dynamic map (LDM) and evaluates the criticality of the situation to make a decision. At the same time, the pedestrian's cell phone receives a warning notification.

# 7 Identified threats

## 7.1 Threats to confidentiality

Threats to confidentiality described in this clause are illustrated in Figure 10.

– Eavesdropping:

  An attacker can sniff (i.e., read and/or record) V2V messages of nearby vehicles and V2I messages of RSUs and then analyze traffic information by processing sniffed messages.

  An attacker can sniff V2D messages between a central communication unit and a nomadic device. The attacker could then analyze dynamic information about the vehicle, such as current location and speed.

  An attacker can sniff V2P messages and mislead pedestrians into a dangerous road situation.

– Leakage of personally identifiable information:

  An attacker can analyze information to discover the owner of a vehicle by collecting its V2X messages and tracking its location on the driving route for a particular person.

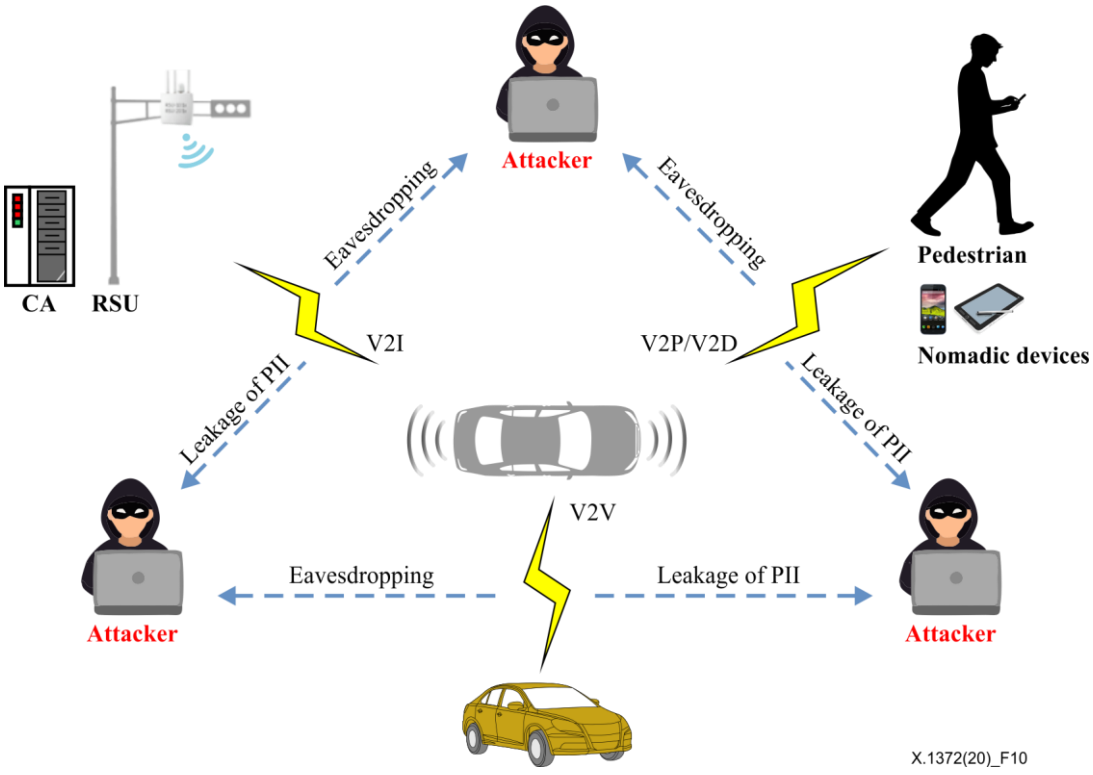



**Figure 10 – Threats to confidentiality**

## 7.2 Threats to integrity

Threats to integrity described in this clause are illustrated in Figure 11.

– Manipulation of routing message:

  A malicious intermediate node modifies the routing message; vehicles will then receive false information.

– Manipulation of credential information:

  Credential manipulation means that the vehicle's private key or ID (identifier) is modified, so an attacker can use another vehicle's credential information without authorization.

– Manipulation of sensor information:

  An attacker can modify the physical address of a communication module or can manipulate ECU information such as that from a speed sensor. Furthermore, there numerous other sensors on a vehicle such as radar and camera as driver assistance equipment. False sensor data including latitude, longitude, elevation, speed, heading, steering wheel angle and acceleration could be delivered to other OBUs or RSUs. This manipulated sensor data can result in traffic disorder. For example, a false acceleration value could make neighboring vehicles turn on their electronic emergency brake lights (EEBLs) to reduce the chance of multiple vehicle collisions, even if the real traffic condition is fine.

– Manipulated application on a nomadic device:

  A manipulated application can have a harmful effect on a vehicle through the V2D communication interface. For example, the manipulated application can force the nomadic device to send a large number of benign messages to the vehicle; this practice is known as message flooding. Furthermore, the manipulated application can inject malicious code into an OBU and send a message that requires many computation resources. The manipulated application can also send a larger number of messages of much bigger size than the storage capacity available on the OBU.

– Replay attack:

  An attacker can intercept V2V messages from nearby vehicles and V2I messages of RSUs. Later, this attacker can replay those messages or information for its malicious purpose.

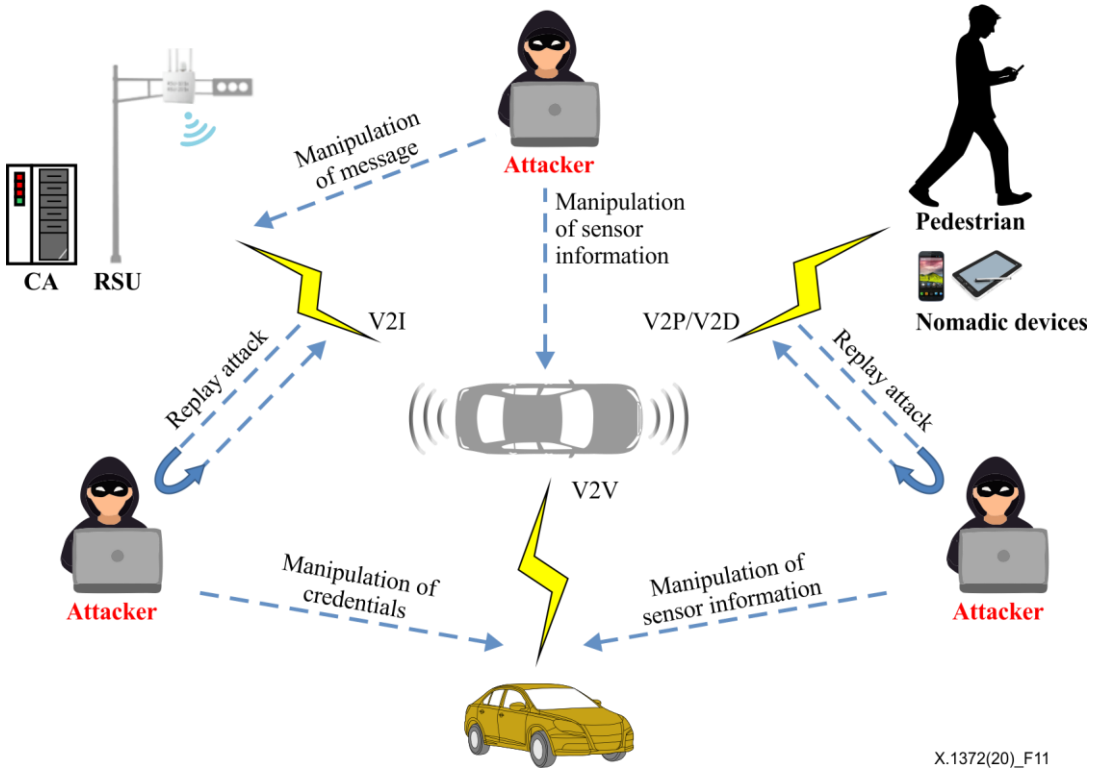



**Figure 11 – Threats to integrity**

## 7.3 Threats to availability

Threats to availability described in this clause are illustrated in Figure 12.

– Jamming and distributed denial of service (DDoS) attack on V2X communication channel:

  An attacker can send many useless messages; this technique is known as message flooding. Forwarding only a specific message by a routing node can be categorized into this attack.

– DDoS attack on OBU:

  An attacker can inject malicious codes into an OBU and send messages that require significant computational resources. This attacker can also send many messages whose size, cumulatively, is bigger than the storage capacity of the OBU. In particular, frequent software updates without authorization are an example of a severe attack of this type.

– Timing attack:

  A timing attack is, for example, the delaying of delivery of safety message to other vehicles. Thus, it may prevent the appropriate V2X communication services such as broadcasting of warning messages.

– Hacking of sensors:

  Sensors might be under attack and cause faults to provide malicious values. In general, there are two fault types that may exist in the sensor: transient fault and permanent fault. Transient fault may occur during the system's normal operation and quickly disappear. In fact, most sensors exhibit a transient fault model that bounds the amount of time in which they provide wrong measurements. For example, it is not uncommon for GPS to temporarily lose connection with satellites (or receive noisy signals), especially in cities with high-rise buildings. Similarly, a sensor transmitting data using an over-utilized network (e.g., with the TCP/IP protocol with retransmissions) may fail to deliver its measurements on time, thus providing incorrect information when the messages arrive. Due to their short duration, however, transient faults should not be considered as a security threat to the system.

In contrast, permanent faults are sensor defects that persist for a longer period of time and may seriously affect the system's operation. For instance, a sensor may suffer physical damage that introduces a permanent bias in its measurements. In such a scenario, unless the fault can be corrected for in the software, the system would benefit from discarding this sensor altogether.

Depending on the attacker's goal, attacks on sensor measurements may manifest either as transient or permanent faults. Each one has benefits and drawbacks for the attacker. Making a sensor behave as if transiently faulty may prevent the attacker from being discovered but also limits his capabilities, whereas a prolonged attack that is similar to a permanent fault may be more powerful but could be detected quickly.

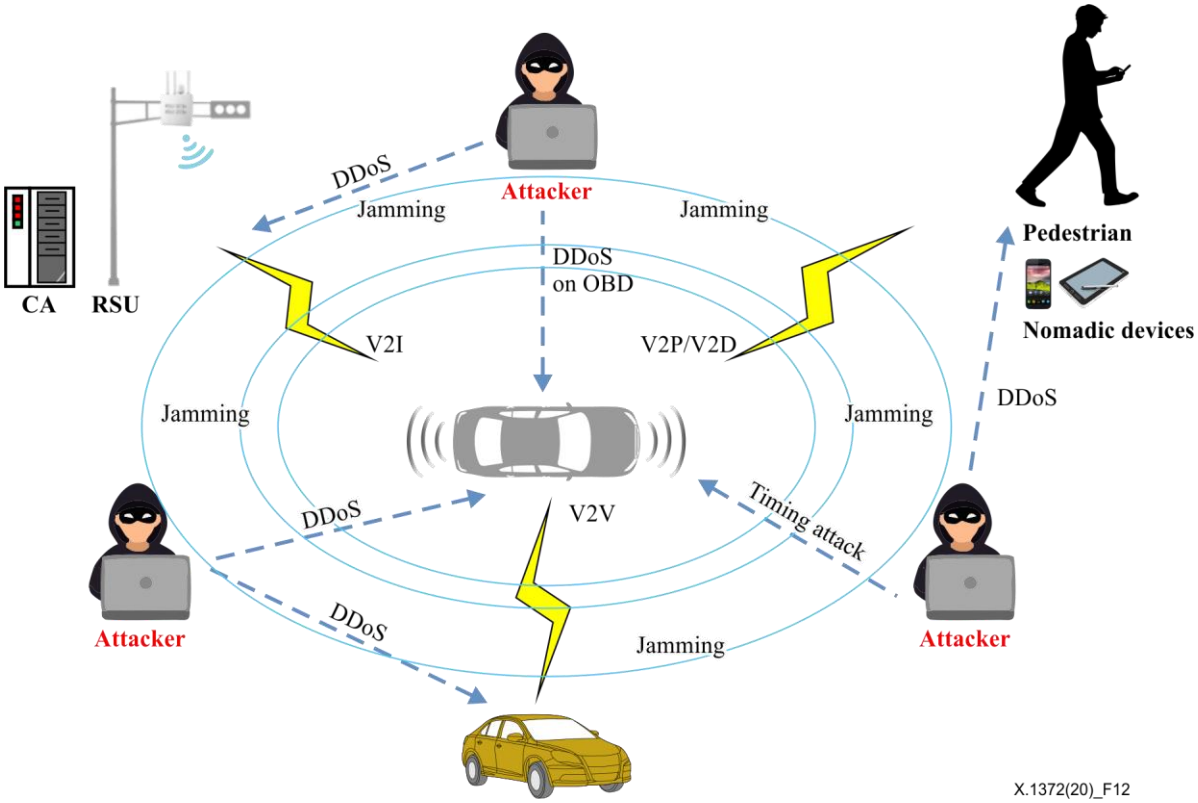



**Figure 12 – Threats to availability**

## 7.4 Threats to non-repudiation

Threats to non-repudiation described in this clause are illustrated in Figure 13.

– Manipulation of certification database:

An attacker can manipulate the pseudonym database in the CA. The attacker can then modify the relation between a long-term certificate and a short-term pseudonym certificate.

– Unauthorized access to credentials:

An attacker can access a private key and a certificate without authorization. If the private key is exposed, then non-repudiation of the vehicle, RSU and nomadic device cannot be provided.

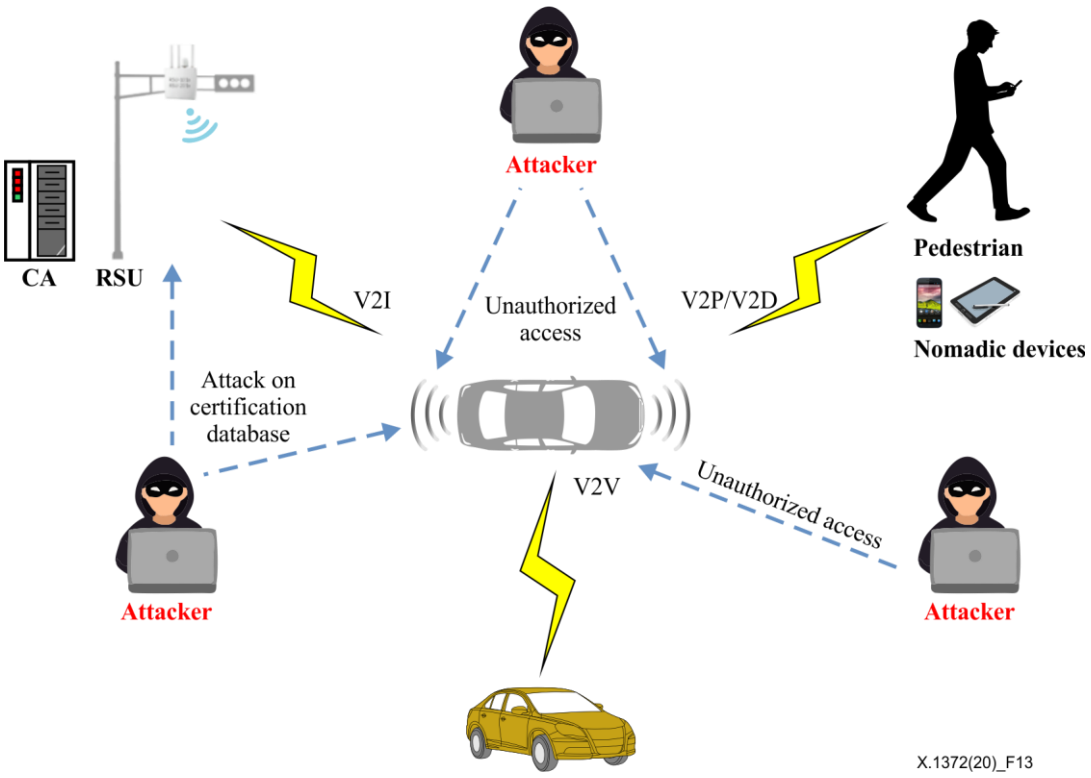



**Figure 13 – Threats to non-repudiation**

## 7.5 Threats to authenticity

Threats to authenticity described in this clause are illustrated in Figure 14.

– Routing table and LDM modification attack:

  An attacker can spoof the GPS information of a vehicle and modify its original geospatial information.

– Impersonation attack:

  An attacker can pretend to be another entity by stealing the other entity's ID information. The attacker can then receive messages normally sent to the other entity and can also send messages as if they were normally generated by the other entity. For example, if the other entity is an emergency vehicle, the attacker can send a message to other surrounding vehicles such as "I am an emergency vehicle. Please move out of my way."

  An attacker also sends a false malfunction signal on behalf of an innocent vehicle; the CA could then revoke the innocent vehicle.

– Sybil attack:

  A Sybil attack can occur when one vehicle simulates multiple vehicles by using multiple vehicle IDs.

– Pseudonym analysis attack:

  An attacker can analyze the relationship between vehicle IDs and pseudonyms to find the multiple pseudonyms used for the same vehicle.

– Manipulation of certification database:

  An attacker can manipulate the pseudonym database in the CA. The attacker can then modify the relation between a long-term certificate and a short-term pseudonym certificate.

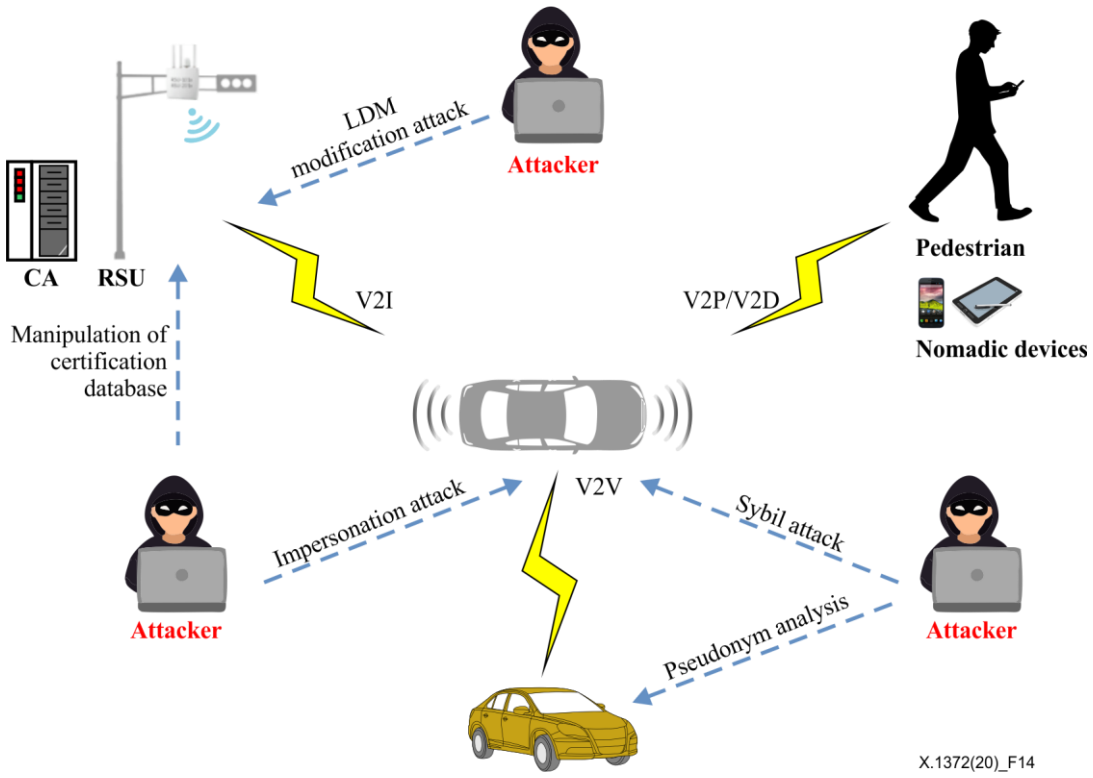



**Figure 14 – Threats to authenticity**

## 7.6 Threats to accountability

Threats to accountability described in this clause are illustrated in Figure 15.

– Unauthorized duplication of a nomadic device:

  Because of some particular services, such as vehicle diagnostics for example, an authorized nomadic device could access the central communication unit in a vehicle. However, if its' authorization is copied by malicious devices, as may result for example when the authorized device's login account has been utilized by another malicious device, then this malicious device could access the communication unit. This central communication unit within a vehicle could be manipulated by an unauthorized nomadic device.

– Unauthorized duplication of a vehicle and RSU:

  After an attacker achieves (duplicates) the IDs of a vehicle and an RSU, the original vehicle and RSU lose their accountability.

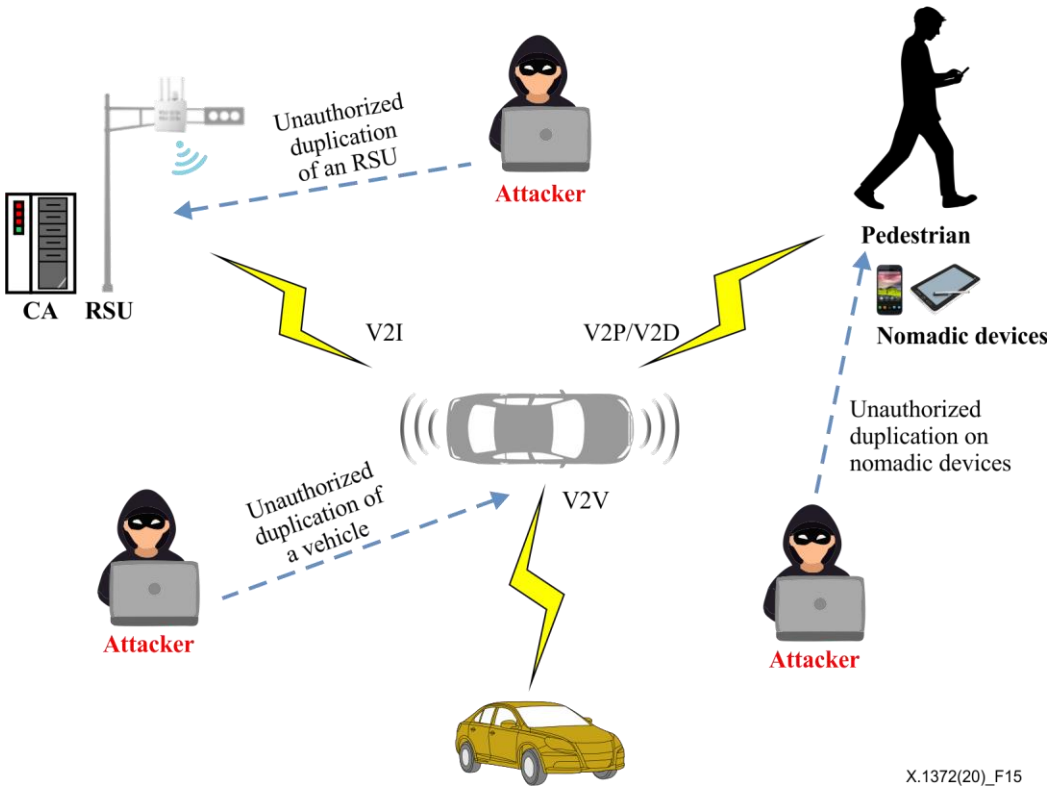



**Figure 15 – Threats to accountability**

## 7.7 Threats to authorization

Threats to authorization described in this clause are illustrated in Figure 16.

– Unauthorized access to safety-sensitive information in a vehicle:

  If there is no authorization control, a malicious user or application can control a vehicle without authorization. For example, the application that plays music through a speaker in a vehicle should not be authorized to access safety-sensitive information such as the vehicle's speed and current status of the brake.

  An unauthorized attacker can also manipulate, erase and overwrite safety-sensitive vehicle data including vehicle parameters such as a threshold of brake and airbag for an emergency situation and system log.

  With regard to an electric vehicle, an unauthorized attacker can manipulate configuration parameters of the vehicle's charging functions.

– Unauthorized access to certain functions in a vehicle using nomadic devices:

  It is critical to define access control functions for nomadic devices that connect to a vehicle. Nomadic devices are generally used as audio, video and navigation tools in the vehicle. It can also display the contents of the nomadic devices on a multimedia head unit. Unauthorized functionality such as communication with a central gateway in the vehicle using this nomadic device can have severe harmful effects on safety.

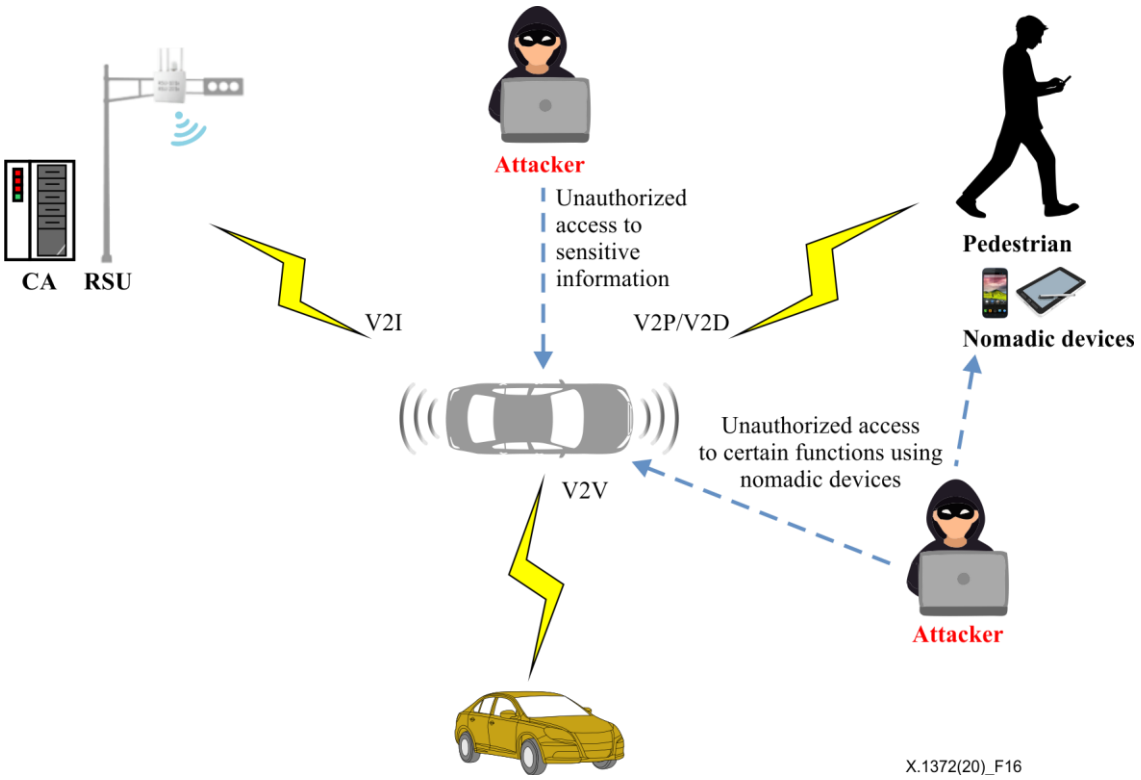



**Figure 16 – Threats to authorization**

## 8 Security requirements

This clause describes security requirements for V2X communication. Clauses 8.1 to 8.7 describe the security requirements in V2X communications, and clause 8.8 provides further detail on these requirements.

### 8.1 Confidentiality

It should not be possible for an unauthorized entity to reveal the messages between vehicles and vehicles, between vehicles and infrastructure, between vehicles and nomadic devices and between vehicles and pedestrians.

It should not be possible for an unauthorized entity to analyze the identification of a person through personally identifiable information (PII) within communication messages such as the location or driving route of a particular person.

### 8.2 Integrity

Messages sent to or from a vehicle, an RSU or a nomadic device should be protected against unauthorized modification and deletion.

### 8.3 Availability

It should be possible for an entity to send and receive messages in appropriate latency. For example, a forward collision-warning message should be transmitted to an incoming vehicle before the vehicle arrives at the accident point. If the warning message cannot be delivered to the incoming vehicle because of a jamming attack, the V2V/V2I safety application could be useless.

It should be possible for an entity to process an exchanged information in real-time, thus requiring the implementation of low-overhead and lightweight cryptographic algorithms.

## 8.4 Non-repudiation

It should not be possible for an entity to deny that it has already sent a message. This requirement can be implemented using digital signatures in V2X communication systems.

## 8.5 Authenticity

Entities such as OBUs and RSUs in a V2V/V2I communication environment should be able to provide proof of being an authorized owner of a legitimate ID. This requirement is known as entity authentication. It is also required between a vehicle and a nomadic device.

In the case of group communication, a vehicle does not need to prove its ID. The vehicle should prove that it is an authentic member of the group. This requirement is called attribute authentication.

## 8.6 Accountability

It should be possible for an entity to detect and/or prevent any misbehavior of OBUs or vehicle sensors by checking their data.

For example, an OBU can check some information in a received message for kinematic sanity against the previously received message. If the position data of a current message shows impossible changes in the vehicle's dynamic behavior, it might be misbehavior of other entity. Consequently, the information can be filtered or ignored.

## 8.7 Authorization

It is critical to define access control and authorization for the different entities. Specific rules should be enforced for accessing or denying specific entities access and/or use of certain functions or data.

## 8.8 Applicability of V2X security requirements

Table 1 lists the security requirements described in clauses 8.1 to 8.7, and their applicability to the various forms of V2X communications.

**Table 1 – Security requirements for V2X communication**

| | **V2V warning propagation** | **V2V platooning communication** | **V2V beaconing** | **V2I warning** | **V2V/V2I information exchange** | **V2D communication** | **V2P communication** |
|---|---|---|---|---|---|---|---|
| Confidentiality (general) | − | O | − | − | O | O | O |
| Confidentiality (PII) | O | O | O | ▲ | O | O | O |
| Integrity | O | O | O | O | O | O | O |
| Availability | O | O | O | O | O | ▲ | O |
| Non-repudiation | O | O | O | O | O | O | O |
| Authenticity | O | ▲ | O | O | O | O | O |
| Accountability | O | O | O | O | O | O | O |
| Authorization | − | O | − | − | O | O | − |

O: Required, −: Not required, ▲: partially required

In a V2V warning propagation situation, confidentiality is not mandatorily required since the exchanged messages from a vehicle to another contain already public information such as traffic accident ahead or the emergency vehicles approaching. In V2V warning propagation situation, the propagated messages do not include any information related to authorization.

In a V2V platooning communication scenario, authentication of the vehicle is partially required which means that each vehicle is not necessarily required to authenticate each vehicle in the group. Entity authentication means the process by which one entity is assured of the identity of the other entity that

is participating in the communication. However, in a V2V platooning scenario, each vehicle does not require exact entity authentication for the group. In such a case, it is sufficient to prove that each vehicle is a member of the group. In other words, the identity of a vehicle is not assured and it is only assured that a vehicle is a member of the group. This kind of authentication can be called attribute authentication. The messages in this scenario also have authorization information such as platoon leader or platoon membership.

In a V2V beaconing scenario, broadcasting information should be protected against unauthorized modification and deletion. However, if the message does not include the vehicle's identification information, the message is not required to be encrypted. Furthermore, Authorization is not required for the V2V beaconing scenario because the broadcasted information will not be used for the aim of controls.

In a V2I warning scenario, the information between a vehicle and an infrastructure such as an RSU is normally traffic information that is shared publicly. That is why the confidentiality in a V2I warning environment is not required. The partially required mark for PII protection in a V2I warning situation means that a vehicle requires PII protection, but an RSU does not require PII protection. A vehicle's current location and travel history should be protected if the driver is linked to the vehicle. However, an RSU has no PII as the RSU is not linked with people.

In a V2D communication scenario, the nomadic device is used in the vehicle. When the nomadic device communicates with the vehicle, availability does not have the same impact as V2V communication scenario because the number of the devices in the vehicle is practically smaller than that of vehicles on the road in real environments.

In a V2P communication scenario, a nomadic device in pedestrians or VRUs cannot have any function that requires the authorization of the vehicle.

## 9 Implementation of V2X communication with security

This clause provides possible implementations of V2X communication to fulfil security requirements such as confidentiality, integrity, availability etc., which are described in clause 8. A brief overview of fundamental cryptographic algorithms suitable for vehicular communication environments is provided, followed by description on how to use them in V2X communication scenarios such as emergency warning and platooning.

### 9.1 Cryptography for entity authentication and message confidentiality

The V2X entity authentication function can be achieved using digital signature algorithms. A message confidentiality function can be implemented using symmetric and public-key cryptographic algorithms. This Recommendation provides example implements these functions. Adaptation and selection of mechanisms and parameters, which are related to the entity authentication and message confidentiality functions, depend on deployment policy.

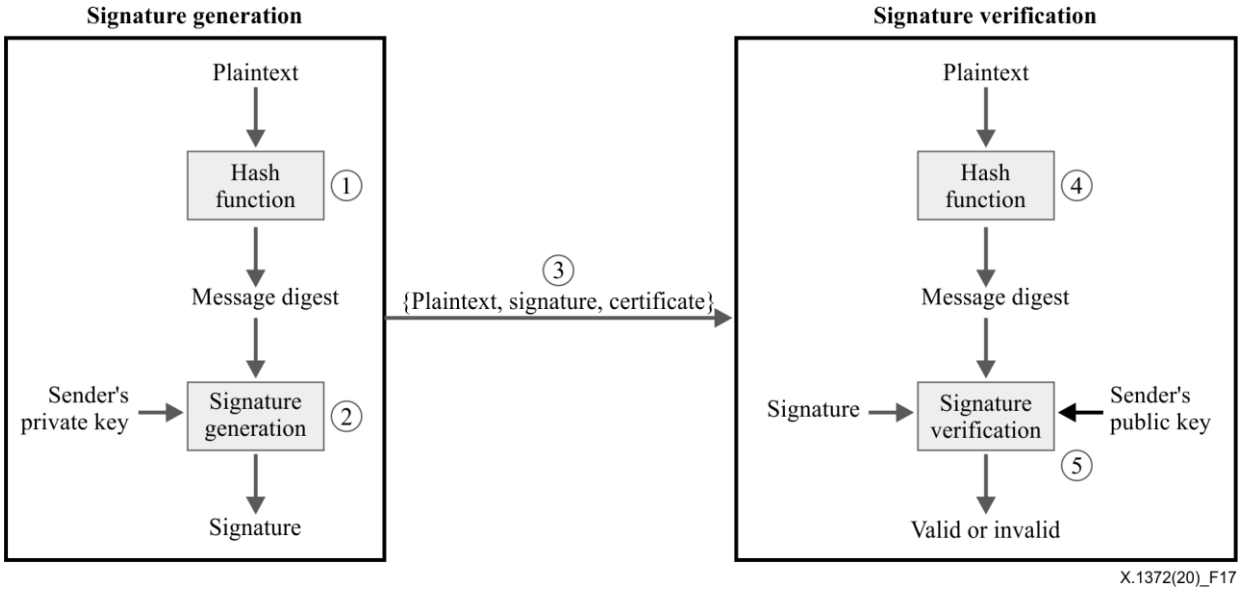



**Figure 17 – Signature generation and verification**

A digital signature algorithm includes a signature generation process and a signature verification process as shown in Figure 17. A signatory uses the generation process to generate a digital signature on data. A verifier uses the verification process to verify the authenticity of the signature. Each signatory has a public and private key. As shown in Figure 17, the private key is used in the signature generation process. The public key of the signatory is used in the signature verification process.

The overall procedure of signature generation and verification is as follows:

– step 1: with a hash function (such as secure hash algorithm-256 (SHA-256)), a message digest is computed over the plaintext message. For instance, the digest is computed over the protocol version, header, payload and the length of the trailer;

– step 2: a signature of the message digest is generated with the sender's private key;

– step 3: the plaintext, the signature, and a sender's certificate are transmitted to a receiver;

– step 4: the receiver computes the message digest using the received plaintext from the sender;

– step 5: the receiver computes a verification value using the message digest in step 4, the received signature, and the sender's public key. If the verification value is the same as the value in the signature, then the received signature is valid. If the verification value is different from the value in the received signature, the signature is invalid.

Elliptic curve digital signature algorithm (ECDSA) can be used as a digital signature algorithm in V2X communication.

Encryption algorithms are used to support confidentiality of the V2X messages. Asymmetric encryption algorithm such as elliptic curve integrated encryption scheme (ECIES) is used to transport of a key for a symmetric-key algorithm such as advanced encryption standard (AES). Encryption procedure of ECIES is described in Figure 18. In Figure 18, ECIES uses the following functions:

– key agreement (KA): Function used for the generation of a shared secret by two entities;

– key derivation function (KDF): Mechanism that produces a set of keys from keying material and some optional parameters;

– encryption: Symmetric key encryption algorithm;

– message authentication code (MAC): MAC generation algorithm.

In Figure 18, the following notations are used:

– ***u***: Sender's private key

– ***U***: Sender's public key
– ***v***: Receiver's private key
– ***V***: Receiver's public key

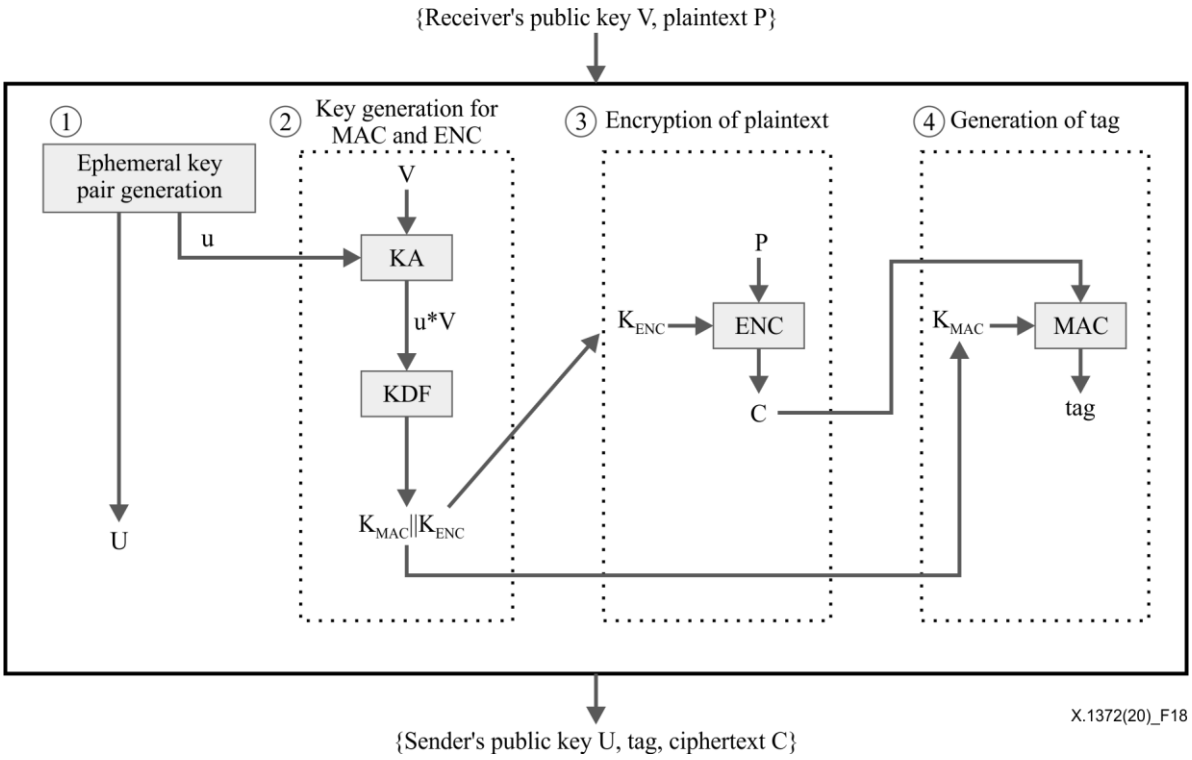



**Figure 18 – ECIES encryption procedure**

As shown in Figure 18, inputs of the encryption procedure are the receiver's public key ***V*** and the plaintext ***P***. Outputs of the encryption procedure are the sender's public key ***U***, tag, and the cipher text ***C***. The message encryption procedure consists of the following steps:

– step 1: Ephemeral key pair generation:

  The sender generates the private key ***u*** and the public key ***U***. It is recommended that the public key ***U*** be freshly generated for each encryption operation;

– step 2: Key generation for MAC and ENC:

  The key agreement function (KA) generates a shared secret by the sender's ephemeral private key ***u*** and the receiver's public key ***V***. The key derivation function (KDF) based on SHA-256 will take this shared secret to generate the concatenation of the message authentication code (MAC) key ($\boldsymbol{K_{MAC}}$) and the encryption key ($\boldsymbol{K_{ENC}}$);

– step 3: Encryption of the plaintext:

  The plaintext ***P*** is encrypted with $\boldsymbol{K_{ENC}}$ using symmetric encryption algorithms.

  ECIES is used to encrypt a symmetric key for encryption of V2X messages using advanced encryption standard-counter mode with cipher block chaining message authentication code (AES-CCM). Therefore, the plain text is actually the encryption key for AES-CCM;

– step 4: Generation of tag

  A MAC function with SHA-256 generates a tag of the cipher text, which is the symmetric key of AES-CCM, in order to support message integrity.

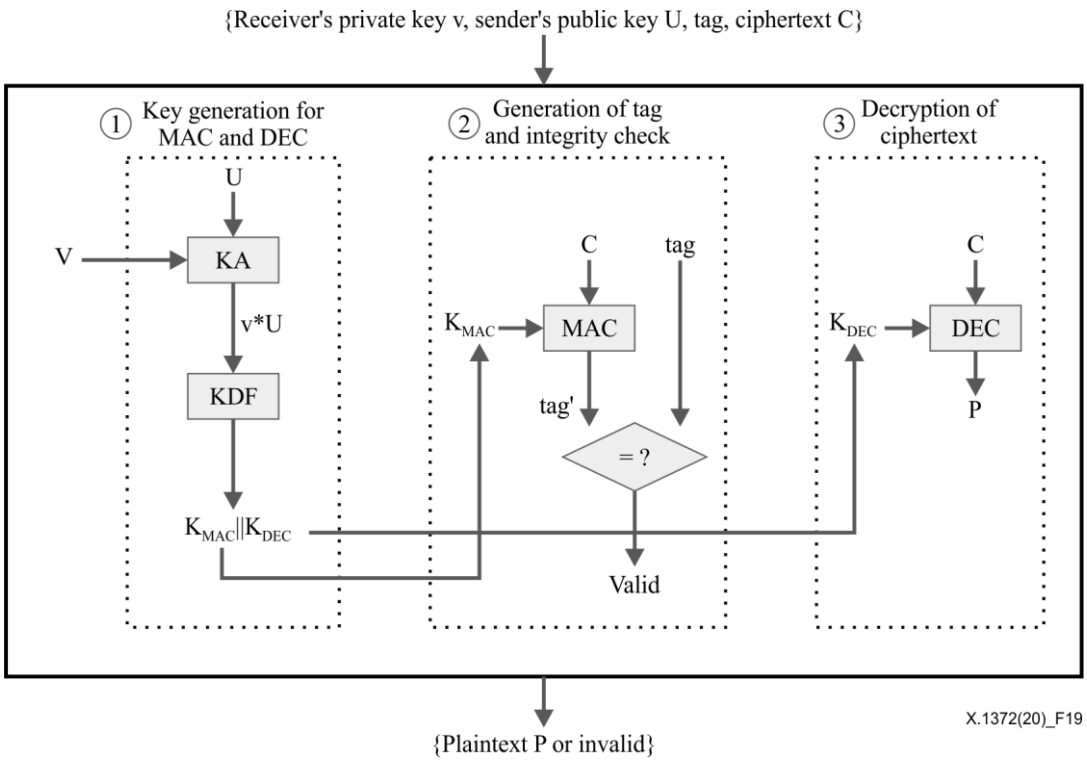



**Figure 19 – ECIES decryption procedure**

Decryption procedure of ECIES is described in Figure 19. As shown in Figure 19, inputs of the decryption procedure are the receiver's private key ***v***, the sender's public key ***U***, tag, and the cipher text ***C***. Outputs of the decryption procedure are the plaintext ***P*** or the results of the message integrity test. DEC, in Figure 19, means decryption procedure of symmetric-key algorithm. The message decryption procedure consists of the following steps:

– step 1: Key generation for MAC and DEC:

  The key agreement function (KA) generates a shared secret by the sender's ephemeral public key ***U*** and the receiver's private key ***v***. The key derivation function (KDF) based on SHA-256 will take this shared secret to generate the concatenation of the message authentication code (MAC) key $K_{MAC}$ and the decryption key $K_{DEC}$. It is noted that $K_{ENC}$ and $K_{DEC}$ are same values in symmetric key algorithms;

– step 2: Generation of tag and integrity check:

  The MAC function generates a tag of the received cipher text ***C*** with $K_{MAC}$. The computed tag' is compared to the received tag. If the values are not identical, the received message is discarded because of failure in message integrity check;

– step 3: Decryption of the cipher text:

  The cipher text ***C*** is decrypted with $K_{DEC}$ using symmetric encryption algorithms.

ECIES is used to encrypt a symmetric key for encryption of V2X messages using AES-CCM. Therefore, the plaintext is actually the encryption key for AES-CCM.

## 9.2 Message confidentiality for emergency road safety warning

A generic use case for emergency warning is shown in Figure 20. The brake ECU sends a message to the V2X communication unit of a vehicle through its central communication unit (CCU). The corresponding ITS application in the V2X communication unit receives the message from the brake ECU and generates a V2X warning message. The generated message is sent to the networking and transport layer. This message should be signed or encrypted by the security layer. Then the physical

layer sends the signed or encrypted message to a wireless communication channel. Using the wireless communication channel, the message is transmitted to the receiver. At the receiver, the message is verified or decrypted by the security layer and finally passed to the upper layer, the corresponding ITS application. The corresponding ITS application can update an LDM or alert a driver with a human interface device and may send a control message to the brake ECU to reduce the speed of the vehicle.

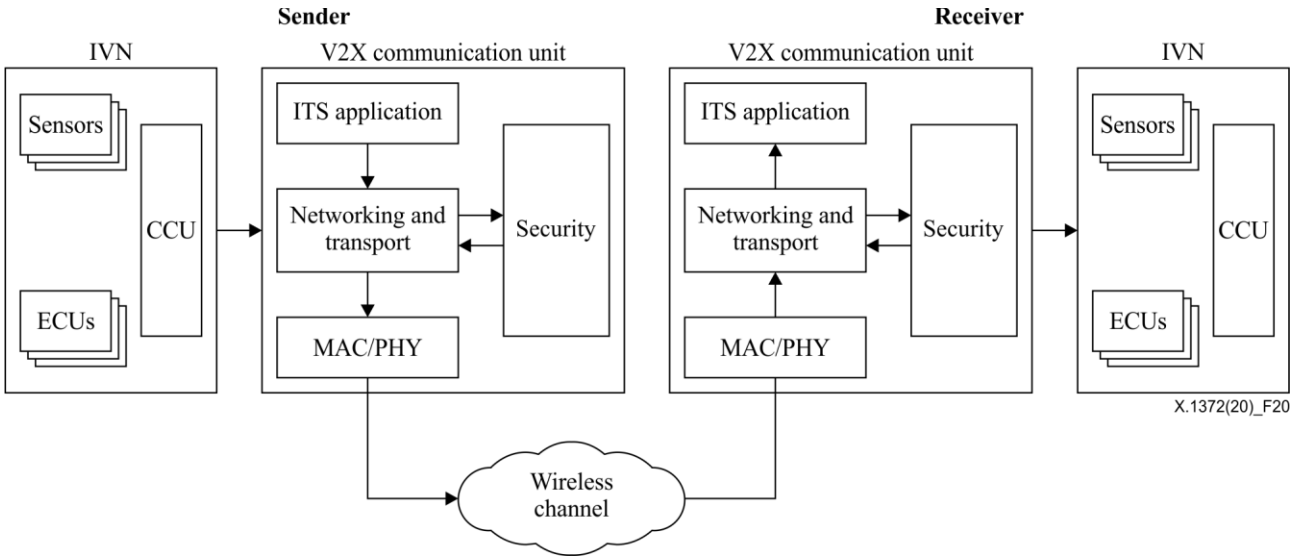



**Figure 20 – Procedure of emergency warning**

## 9.3 Entity authentication for vehicle platooning

Platooning is an effective approach that changes a driving pattern from individual driving to platoon-based driving. In general, platoon-based driving involves a group of vehicles with common interests, where one vehicle follows another and maintains a small, almost constant distance from the preceding vehicle, forming a platoon, as shown in Figure 21. As pertains to platooning, there are three major processes: platoon merging, platoon cooperation/maintenance, and platoon splitting.

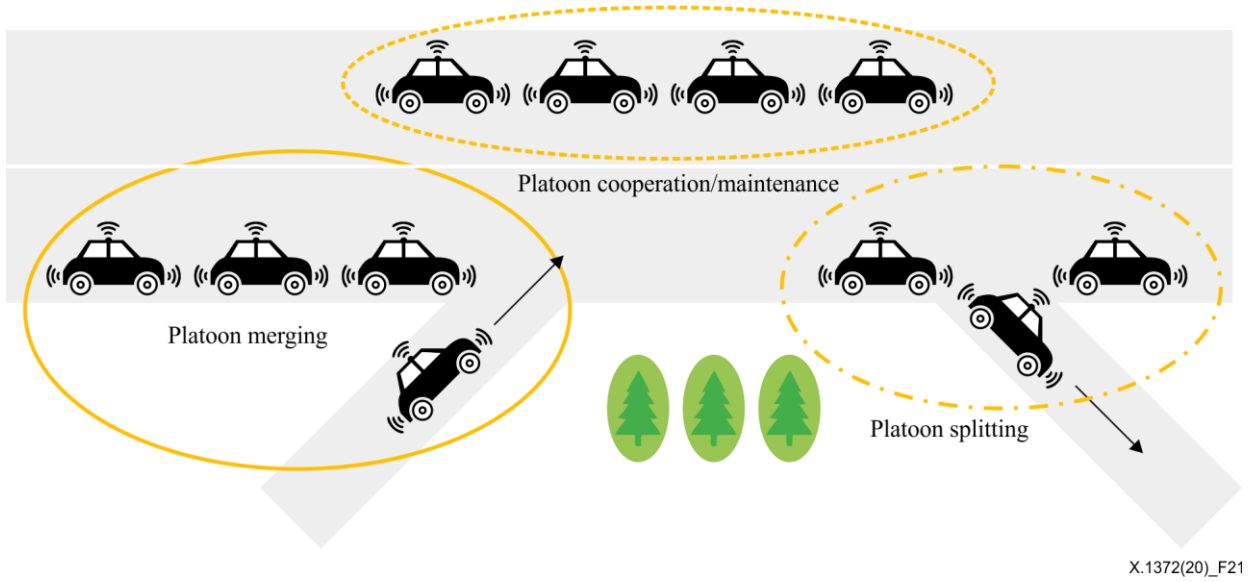



**Figure 21 – Use case of platooning**

– platoon merging: the vehicle, which is not a member of a platoon, will move and merge into the platoon at the road intersection ahead;
– platoon cooperation/maintenance: vehicles within the same platoon need to communicate and cooperate with each other to maintain the platoon and achieve tasks such as making way for higher priority vehicles, adjusting their positions based on route planning, crossing traffic junctions and lane switching;
– platoon splitting: the vehicle will be splitting from its platoon into another lane at the road intersection ahead.

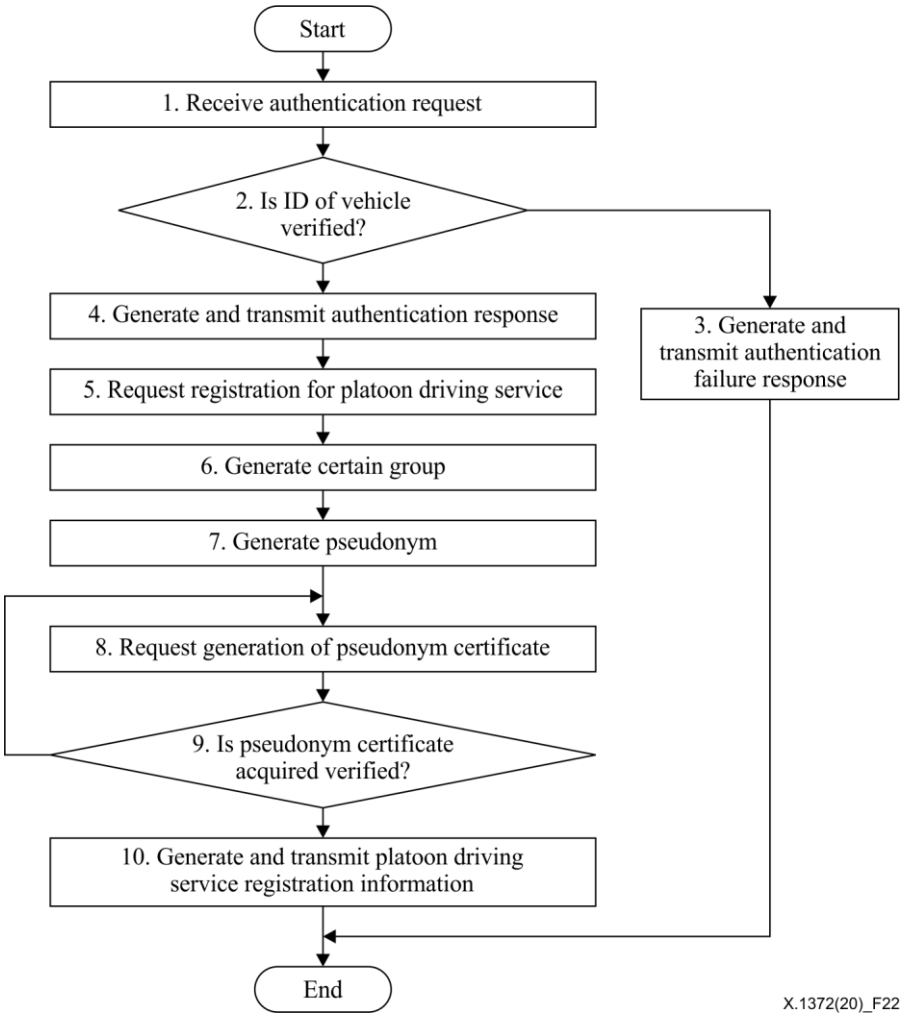



**Figure 22 – Platoon registration procedure**

An example of authentication for a platoon driving service is shown in Figure 22. Referring to Figure 22, if an authentication request for the registration of a group driving service, i.e., a vehicle authentication request, is received from a vehicle in a service execution mode in step 1, the ID of the vehicle should be verified, e.g., using a digital signature algorithm of a public key crypto system, in step 2. Herein, the authentication request of the vehicle may be performed in a manner of transmitting a message signed with a private key of the vehicle to the group driving service system. As a result of the verification in step 2, if the ID of the vehicle is determined to be invalid, the group driving service system generates a corresponding authentication failure response and transmits this response to the vehicle, as shown in step 3.

As the result of the verification in step 2, if the ID of the vehicle is determined to be valid, the group driving service system generates an authentication response for the vehicle and transmits this response to the vehicle, as shown in step 4.

Thereafter, when the authentication response is received, i.e., the authentication of the vehicle is achieved, after a user inputs and selects group driving registration information including group driving qualification, starting place, destination, estimated time of departure, estimated time of arrival and desired resting place, the vehicle transmits the group driving registration information to the group driving service system to thereby request the registration of the group driving service, as shown in step 5.

Subsequently, if a request for the registration of the group driving service, which includes the group driving registration information, is input from the vehicle, the group driving service system generates a certain group using the group driving registration information such as the same destination, the same starting place, the same estimated time of arrival, and so on, and then stores/registers information on the certain group in the group information, as shown in step 6.

Herein, the certain group may include at least one group leader, i.e., a leader vehicle, and at least one member, i.e., a member vehicle. After that, group driving service system assigns a pseudonym to each vehicle in the certain group, as shown in step 7, generates a certificate request message for requesting the generation of a pseudonym certificate for the pseudonym assigned to each vehicle in the certain group, and transmits the certificate request message to the authentication centre, as shown in step 8.

The group driving service system monitors whether or not the pseudonym certificate is acquired from the authentication centre in step 9. As a result of the monitoring, if the pseudonym certificate is secured, the group driving service system stores the pseudonym certificate in the group information DB. The pseudonym certificate may be a digitally signed message of the authentication centre. It is possible to guarantee the justification of the pseudonym through the pseudonym certificate. The pseudonym is a public key assigned to each vehicle by the group driving service system.

A plurality of pseudonyms may be assigned to each vehicle. Since the pseudonym does not have information associated with an ID of each vehicle, the ID of the vehicle participating in the group driving is not exposed, so that it is possible to protect the PII of each vehicle participating in the group driving.

If the notification is received thereto, the group driving service system generates group driving service registration information for the certain group, stores the same in the group information DB, and transmits the same to each vehicle in the certain group in step 10. Herein, the group driving service registration information may include a group ID, a pseudonym assigned to each vehicle, a pseudonym certificate for the pseudonym, and so on. Each vehicle, i.e., a user of the vehicle, in the certain group for which the group driving service is registered can accomplish the group driving by performing communications between vehicles in the certain group using the group driving service registration information provided from the group driving service.

### 9.4 Vehicular PKI

A public-key infrastructure (PKI), that facilitates and manages digital certificates, is necessary for building trust among participants in vehicular communication environments. Vehicular PKI is distinguished from the conventional PKI in several aspects. The most important aspect is using pseudonyms in order to protect the exposure of a vehicle's location related to the owner's location. The number of certificates is huge compared to the conventional PKI. Therefore, the main objective of vehicular PKI is to provide efficient methods for requesting certificates and handling revocation.

Appendix II describes reference models for vehicular PKI in more details.

# Appendix I

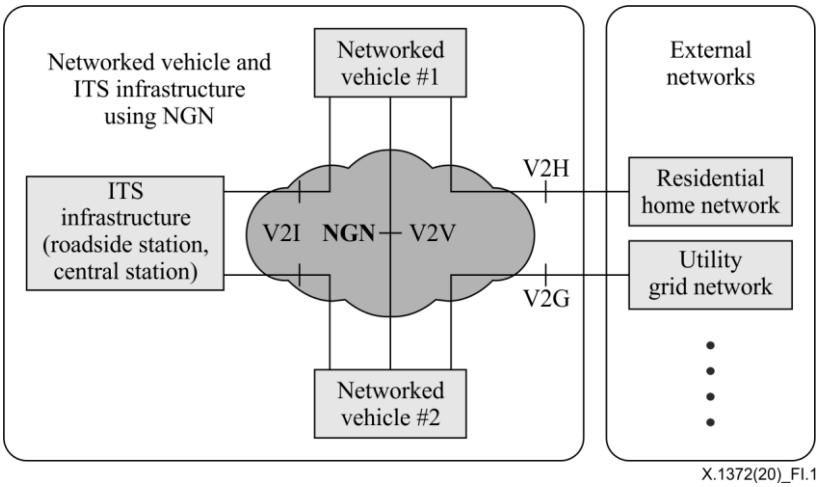
## Reference models for vehicular communication

(This appendix does not form an integral part of this Recommendation.)

### I.1 ITU-T framework of networked vehicle services and applications using NGN

The framework of networked vehicle services and applications in the context of next-generation networks (NGN) is described in [b-ITU-T Y.2281]. A vehicle is one of the important components utilizing network capabilities in terms of the vehicle to infrastructure (V2I), vehicle to vehicle (V2V) and vehicle to home (V2H) communications. In that context, a networked vehicle can cooperate with next-generation networks (NGNs) to support more advanced services and applications such as road safety applications, road traffic-related applications, multimedia services and location-based implementation of these services.

[b-ITU-T Y.2281] identifies the relationship between NGN and a networked vehicle as well as requirements taking into consideration the necessity of supporting networked vehicle services and applications using NGN. In addition, a framework architecture of NGN-capable networked vehicle and intelligent transport systems (ITS) infrastructure is described to support the communication features of an NGN harmonized with the networked vehicle.

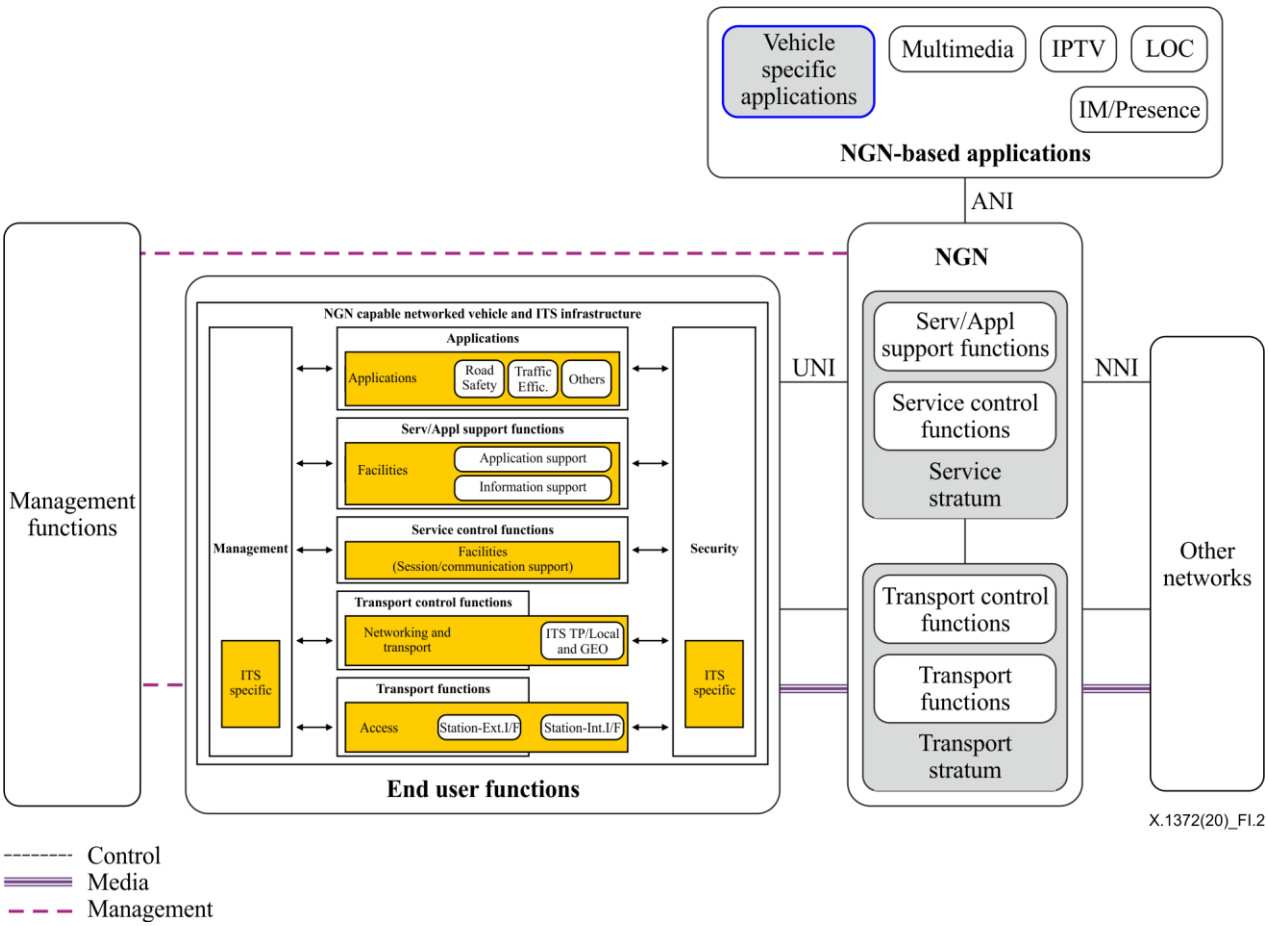



NOTE – Figure source [b-ITU-T Y.2281].

**Figure I.1 – Overall configuration model of networked vehicle and ITS infrastructure**

Figure I.1 shows a configuration model of ITU-T Y.2281 and shows how networked vehicles relate to the ITS infrastructure and also to external networks which include residential home networks and a utility grid network for power transmission using NGN. In comparison with other ITS standards, [b-ITU-T Y.2281] is focused on the use of NGN in ITS environments. [b-ITU-T Y.2281] identifies the use of NGN in ITS environments in order to minimize interoperability problems between peer-to-peer ITS communication and a public network. These interoperability features are especially important in the support of quality of service (QoS), mobility, and security with various multimedia services.

Figure I.2 shows an overview architecture of NGN-capable networked vehicle and ITS infrastructure in cooperation with NGN. NGN is composed of "end-user functions", "service stratum", "transport stratum", "management stratum" and "NGN-based applications". The function of NGN-capable networked vehicle and ITS infrastructure is located at the end-user functions in view of NGN. [b-ITU-T Y.2281] describes how the vehicle-specific NGN applications such as emergency call are supported through NGN.




NOTE – Figure source [b-ITU-T Y.2281].

**Figure I.2 – Overview architecture of NGN-capable networked vehicle and ITS infrastructure in cooperation with NGN**

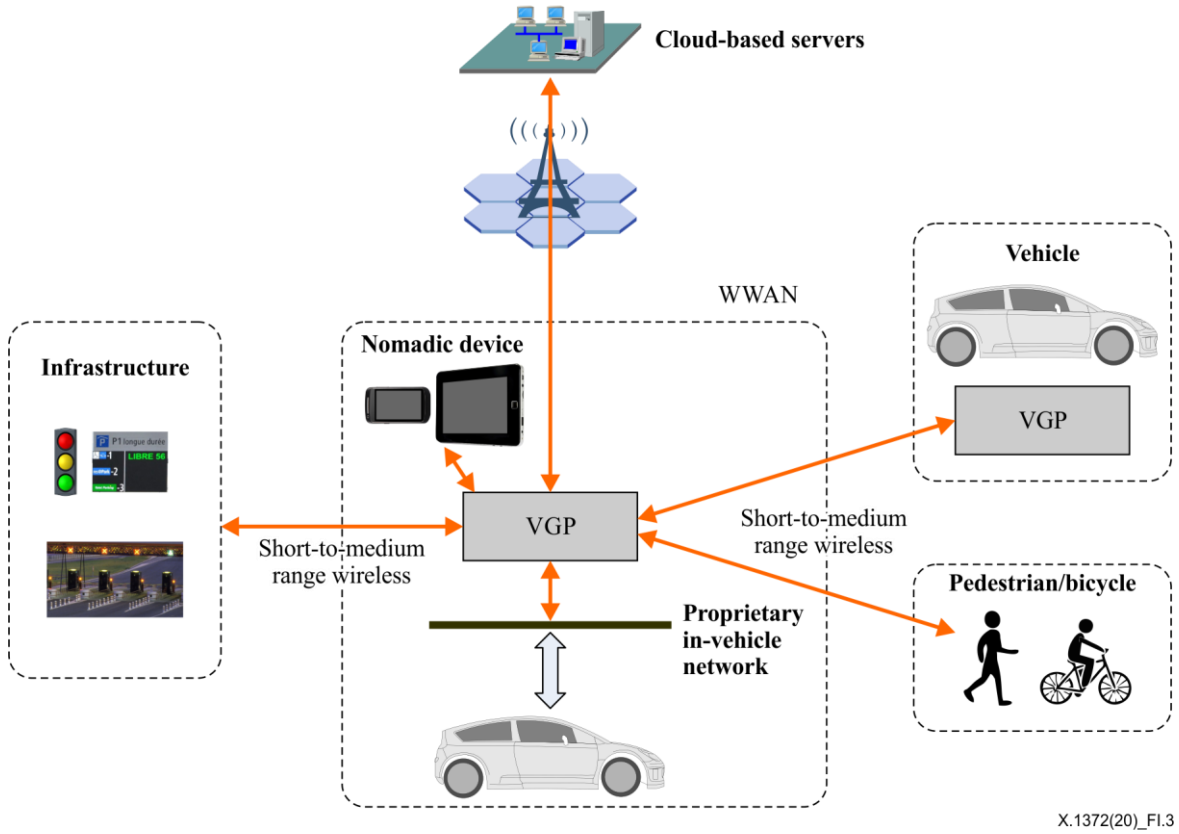
Security considerations of [b-ITU-T Y.2281] refer to [b-ITU-T Y.2201]. Security considerations are required according to the network which is connected to the networked vehicle. However, [b-ITU-T Y.2281] only specifies the security consideration of NGN and other cases of security requirements are out of the scope of [b-ITU-T Y.2281].

The ITU-T framework of networked vehicle services and applications using NGN is focused on the adaptation of NGN to the vehicular environment. [b-ITU-T Y.2281] does not specify security aspects of the vehicular environment. IEEE wireless access in vehicular environments (WAVE) architecture, described in [b-IEEE WAVE], is focused on a 5.9 GHz radio interface since it does not explicitly include an application to communicate with another network. ETSI ITS architecture, described in [b-ETSI EN 302 665], refers to the application layer which is a protocol stack for communication. Considering that the access layer includes IEEE 802.x, 3G cellular and Bluetooth, ETSI ITS architecture is intended to support multiple network protocol stacks.

## I.2 ITU-T Architecture and functional entities of vehicle gateway platforms

Architecture and functional entities of the vehicle gateway platform (VGP) are studied in ITU-T Study Group 16. The architecture, functional architecture framework and functional entities of vehicle gateway platforms are described in [b-ITU-T H.550]. The term of VGP is defined [b-ITU-T F.749.1]. A VGP is the collection of ICT hardware and software in a vehicle operating as an open platform to provide an integrated runtime environment for delivering the communications services of a vehicle gateway. The VGP may also provide higher layer communications services such

as interaction with the driver through the driver-vehicle access services and so on. The subsystems dedicated solely to vehicle operation are not considered part of the VGP.




NOTE – Figure source [b-ITU-T H.550].

**Figure I.3 – Location of VGP in the ITS reference model**

Figure I.3 shows VGP positioning in the intelligent transport system (ITS) reference model: there are six major scenarios, i.e., vehicle to vehicle, vehicle to infrastructure, vehicle to a cloud-based server, vehicle to the nomadic device, vehicle to pedestrian/bicycle and interaction with in-vehicle network scenarios.

– the vehicle to vehicle (V2V) scenario mainly describes the safety and auto-driving scenarios in which vehicles communicate with each other;

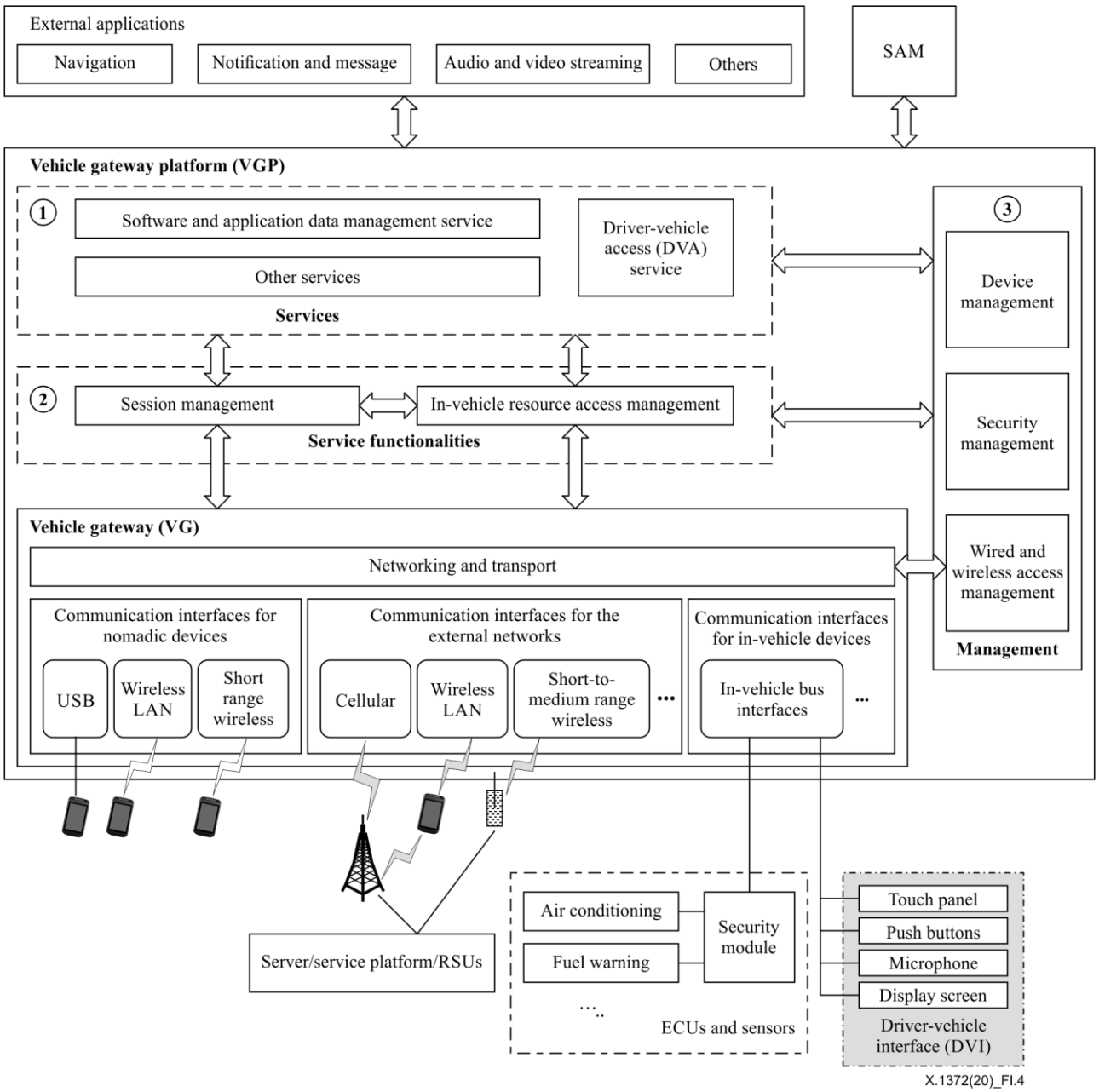
– the vehicle to infrastructure (V2I) scenario mainly describes the safety, electronic toll collection (ETC) and traffic information exchange scenarios in which vehicles communicate with roadside infrastructures;

– the vehicle to cloud-based server scenario mainly describes the emergency call and telematics scenarios in which vehicles communicate with cloud-based services;

– the vehicle to nomadic device scenario mainly describes the telecommunication and remote user interface (UI) scenarios in which vehicles connect to nomadic devices;

– the vehicle to pedestrian/bicycle scenario mainly describes the safety warning scenarios in which vehicles communicate with the devices carried by pedestrian/bicycles;

– interaction with the in-vehicle network scenario mainly describes the vehicle diagnostics, remote data collection and vehicle remote control scenarios in which a VGP communicates with the proprietary in-vehicle network.




NOTE – Figure source [b-ITU-T H.550].

**Figure I.4 – High-level architecture of a VGP**

Figure I.4 presents the high-layer architecture of the VGP. The VGP services include software and an application data management service, driver-vehicle access service, and other services (see block (1) in Figure I.4). Service functionalities include session management and in-vehicle resource access management (see block (2) in Figure I.4). Management includes device management; security management and wired and wireless access management (see block (3) in Figure I.4). Services support external applications such as navigation and infotainment to accomplish the session establishment, data format conversion and specific processing.

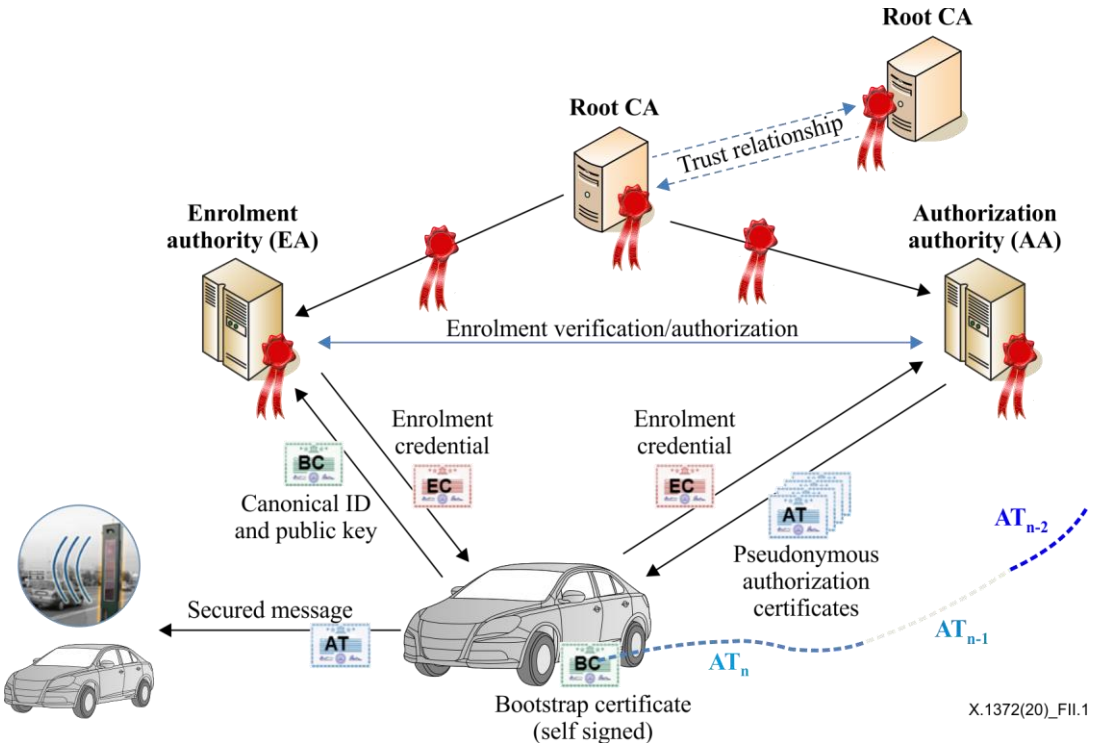
Security aspect on the VGP is described as a part of the management layer in [b-ITU-T H.550]. Generic description of security function is contained in clause 8.4.1 of [b-ITU-T H.550], "Security management". It consists of security management for access layer ,which includes transport and network layer, and security management for services/applications.

# Appendix II

## Reference models for vehicular PKI

(This appendix does not form an integral part of this Recommendation.)

Current ITS communication security functionalities include message authentication, which has an impact on the privacy of vehicles and drives. At the European level, the European Telecommunication Standards Institute (ETSI) has defined a message authentication mechanism based on the use of a public key infrastructure as the vehicular PKI as illustrated in the Figure II.1.




NOTE – Source [b-ETSI TS 102 940].

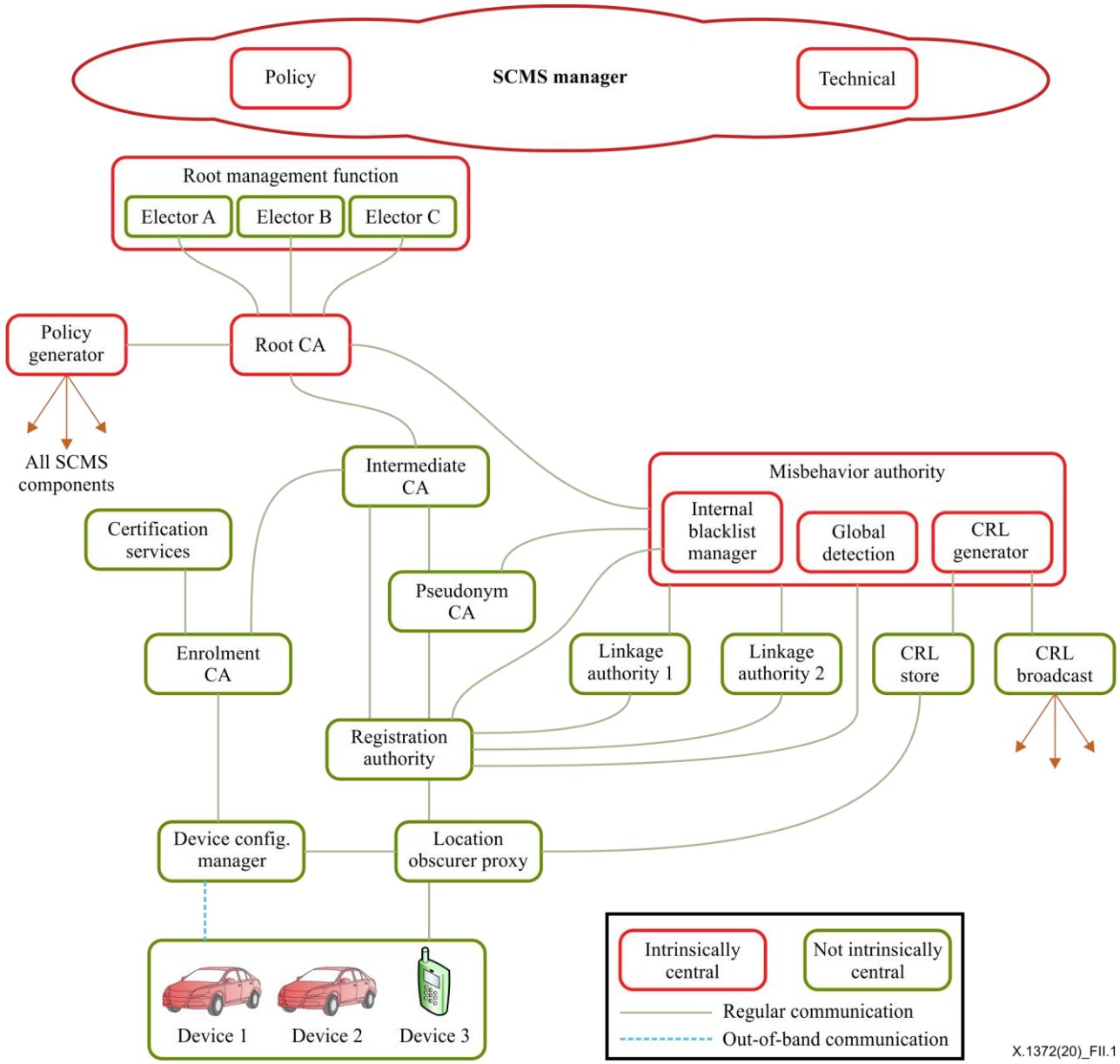
**Figure II.1 – Vehicular PKI in ETSI (Source: [b-ETSI TS 102 940])**

The root certificate authority (RCA) is the start point of the certificate trust chain; it signs the certificates of other authorities such as an authorization authority (AA) and an enrolment authority (EA), and produces and maintains the certificate revocation list (CRL), the list of revoked authorities. In an operational context, an RCA is managed by an actor who can guarantee a high and stable confidence level and who is sufficiently federative, e.g., with a state or a group of states. The EA is the authority that delivers enrolment certificates (ECs) and validates authorization ticket (AT) requests. The AA is a trusted third-party that provides ATs to ITS stations. The AA does not know the ITS station identity and relies on the EA to check whether the ITS station is authorized or not to have the AT. The AT request contains the identity of the EA where the ITS station is registered.

This architecture is meant to provide privacy to ITS stations and avoid tracking; the EA knows the ITS station identity but does not know the pseudonym certificates (ATs) it uses, while the AA knows the ITS station pseudonym certificate but does not know its identity. An ITS station registers itself to the EA and obtains an EC. The EC is used to request pseudonym identities (ATs) to the AA; when an ITS station requests an AT, it sends in the request message its identity encrypted with the EC and the EA identity. The AA receives the pseudonym request, reads the EA identifier and checks the EA

access point to validate the AT request. The EA checks the ITS station EC and validates (or not) the requests. If the request is validated, the AA generates and sends the AT to the ITS station.

On the other hand, the crash avoidance metrics partnership (CAMP) presented a security credential management system (SCMS) for securing V2X communication (see [b-SCMS]). This is based on PKI for V2X security and it is currently transitioning from research to proof-of-concept. The SCMS supports bootstrapping, certificate provisioning, misbehaviour reporting and revocation.




NOTE – Source [b-SCMS].

**Figure II.2 – V-PKI architecture in CAMP**

Figure II.2 presents an overview of SCMS architecture. The relationships amongst different SCMS components are expressed as lines, and it indicates each component sending information or certificates to others.

The major components of the SCMS are as follows:

– enrolment CA (ECA): issues enrolment certificates for a device and can be used to request pseudonym certificates for different geographic regions, manufactures, or device types;

– intermediate CA (ICA): a secondary CA to prevent the root CA from heavy traffic load, and its certificate is issued by the root CA;
– linkage authority (LA): generates pre-linkage values to form linkage values that put in the certificates for efficient revocation. Moreover, the splitting LAs are designed to prevent the operator of an LA from linking certificates belonging to a particular device;
– location obscurer proxy (LOP): changes source address to hide the location of requesting device and prevent linking of network addresses to locations;
– misbehaviour authority (MA): receives and processes misbehaviour reports from devices to identify the potential misbehaviour or malfunctioning. In addition, it will revoke a device's certificate and put it to the CRL. MA also initiates the process of linking a certificate identifier to corresponding enrolment certificates and putting it to the RA's internal blacklist;
– policy generator (PG): maintains the updates of the global policy file for the RA. The global policy file contains global configuration information, and the global certificate chain file, which contains all trust chains of the SCMS;
– pseudonym CA (PCA): issues the short-term pseudonym, identification, and application certificates to devices. Each PCA is limited to a particular geographic region, a particular manufacturer, or a type of device;
– registration authority (RA): validates and processes requests from the device, and it ensures that revoked devices are incapable of issuing new pseudonym certificates. Additionally, RA does not issue more than one set of certificates for a given time period to a device. Moreover, RA will shuffle the requests or reports before sending pseudonym certificate signing requests to the PCA or forwarding information to MA;
– root certificate authority (RCA): the root and top of a certificate chain in the SCMS. It issues certificates for ICAs, PG, and MA.

# Bibliography


[b-ITU-T F.749.1] Recommendation ITU-T F.749.1 (2015), *Functional requirements for vehicle gateways*.

[b-ITU-T H.550] Recommendation ITU-T H.550 (2017), *Architecture and functional entities of vehicle gateway platforms*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.641] Recommendation ITU-T X.641 (1997), *Information technology – Quality of service: framework.*

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.813] Recommendation ITU-T X.813 (1996), *Information technology – Open Systems Interconnection – Security frameworks in open systems: Non-repudiation framework.*

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T X.1371] Recommendation ITU-T X.1371 (2019), *Security threats to connected vehicles*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*.

[b-ITU-T Y.2281] Recommendation ITU-T Y.2281 (2011), *Framework of networked vehicle services and applications using NGN*.

[b-ETSI EN 302 665] ETSI EN 302 665 V1.1.1 (2010-09), *Intelligent Transport Systems (ITS); Communications Architecture*.
<https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf>

[b-ETSI TS 102 940] ETSI TS 102 940 V1.3.1 (2018-04), *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management*.
<https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf>

[b-IEEE WAVE] IEEE Std. 1609.2 (2016), *IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages.*

[b-ISO 13185-1] ISO/TR 13185-1:2012, *Intelligent transport systems – Vehicle interface for provisioning and support of ITS services – Part 1: General information and use case definition*.

[b-OVERSEE] Open Vehicular Secure Platform, OVERSEE Project. (Website).
<https://www.oversee-project.com/>

[b-RITA] United States Department of Transportation, FHWA-JPO-11-130 (2011), *An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues*.
<https://rosap.ntl.bts.gov/view/dot/3334/Share>

[b-SCMS] Crash Avoidance Metrics Partners (CAMP LLC) Vehicle Safety Communications 5 (VSC5) Consortium, *Security Credential Management*

*System Proof-of-Concept Implementation, EE Requirements and Specifications Supporting SCMS Software Release 1.1, 04*. May. 2016. <https://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf>

[b-UNECE GRVA] United Nations Secretary of the Informal document GRVA-01-17, *Draft recommendation on cyber security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA*.

[b-US DOT] United States Department of Transportation, Safety Pilot Program. <https://www.its.dot.gov/research_archives/safety/safety_pilot_plan.htm>

[b-USDOTHS812014] United States Department of Transportation, National Highway Traffic Safety Administration, DOT HS 812 014 (2014), *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*. <https://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf>

[b-US GOV] United States Senator for Massachusetts, Edward J, Markey, Staff Report (2015), *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*. <http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf>

## SERIES OF ITU-T RECOMMENDATIONS

| | |
|---|---|
| Series A | Organization of the work of ITU-T |
| Series D | Tariff and accounting principles and international telecommunication/ICT economic and policy issues |
| Series E | Overall network operation, telephone service, service operation and human factors |
| Series F | Non-telephone telecommunication services |
| Series G | Transmission systems and media, digital systems and networks |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| Series J | Cable networks and transmission of television, sound programme and other multimedia signals |
| Series K | Protection against interference |
| Series L | Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant |
| Series M | Telecommunication management, including TMN and network maintenance |
| Series N | Maintenance: international sound programme and television transmission circuits |
| Series O | Specifications of measuring equipment |
| Series P | Telephone transmission quality, telephone installations, local line networks |
| Series Q | Switching and signalling, and associated measurements and tests |
| Series R | Telegraph transmission |
| Series S | Telegraph services terminal equipment |
| Series T | Terminals for telematic services |
| Series U | Telegraph switching |
| Series V | Data communication over the telephone network |
| **Series X** | **Data networks, open system communications and security** |
| Series Y | Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2020