ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1383 (03/2023)

SERIES X: Data networks, open system communications and security

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

Security requirements for categorized data in vehicle-to-everything (V2X) communication

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 (1)	X.1140–X.1149
Application Security (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.1350–X.1369
Intelligent transportation system (ITS) security	**X.1370–X.1399**
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
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
Cyber Defence	X.1590–X.1599
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
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1383

Security requirements for categorized data in vehicle-to-everything (V2X) communication

Summary

Data security is one of the most important considerations for vehicle-to-everything (V2X) communication. However, in a resource constrained environment such as in-vehicle communication, data protection consumes a lot of resources since cryptographic functions are required.

Recommendation ITU-T X.1383 categorizes the data used in V2X communication into several types such as object attribute data, vehicle status data, environmental perception data, vehicle control data, application service data and user personal data, and assigns three security levels for the categorized data types. Based on these categorized data types and assigned data security levels, this Recommendation provides security requirements for categorized data in V2X communication.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X.1383	2023-03-03	17	11.1002/1000/15108

Keywords

Categorized data, data security, V2X communication.

[*] 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 not received notice of intellectual property, protected by patents/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1383

Security requirements for categorized data in vehicle-to-everything (V2X) communication

1 Scope

This Recommendation categorizes the data used in vehicle-to-everything (V2X) communication into several types and defines the security level for each categorized data type. Based on these categorized data types in each security level, this Recommendation provides security requirements for categorized data in V2X communication.

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.

[ITU-T X.1641]	Recommendation ITU-T X.1641 (2016), *Guidelines for cloud service customer data security*.
[ITU-T X.1603]	Recommendation ITU-T X.1603 (2018), *Data security requirements for the monitoring service of cloud computing*.
[ITU-T X.1372]	Recommendation ITU-T X.1372 (2020), *Security guidelines for vehicle-to-everything (V2X) communication.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 data desensitization [b-ITU-T X.1217]: A process to hide the sensitive data.

3.1.2 data lifecycle [b-ITU-T X.1751]: The entire survival process after data are generated, including data collection, data transmission, data storage, data usage (covering data analysis and visualization), data sharing and data destruction.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABS	Anti-skid Braking System
BSM	Basic Safety Message
CAM	Cooperative Awareness Message
DoS	Denial of Service
GDPR	General Data Protection Regulation
ICV	Intelligent Connected Vehicle

TLS	Transport Layer Security
V2I	Vehicle-to-Infrastructure
V2D	Vehicle-to-nomadic Device
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything

5 Conventions

This Recommendation uses the following conventions:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**should**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keyword "**can**" indicate an optional requirement which is permissible, without implying any sense of being recommended.

The keywords "**should not**" indicates a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

6 Data lifecycle in V2X communication

6.1 Data lifecycle

Data lifecycle is defined based on the data flow in the relevant organization businesses in a vehicle-to-everything (V2X) communication environment. Based on the actual situation in V2X communication, the data security lifecycle is similar to that presented in [ITU-T X.1641], which includes the stages described below of data collection, data transmission, data storage, data usage, data migration, data destruction and data backup and restoration:

– **Data collection**: The process of generating new data in the system within the organization and collecting data from the outside. There are two forms of data collection in V2X communication, one is the data generated in various V2X communication business processes and the other is the data collected by related users, partners and other third parties.

– **Data transmission**: The process in which data flows from one entity to another within the organization. Data transmission in V2X communication mainly involves the realization of data flow between systems and equipment related to V2X communication services.

– **Data storage**: The process of physical storage or cloud storage of data in any digital format. This stage typically occurs nearly simultaneously with the data collection.

– **Data usage**: A series of activities conducted by organizations for dynamic data in V2X communication, such as data query, analysis and processing. In this stage, data update and new data production will be involved.

– **Data migration**: The process of transferring data to external third parties. It includes data display and provision to users in V2X communication. It also includes the process of providing data to each other in cooperation between enterprises and institutions in V2X communication.

– **Data destruction**: The process to make data permanently or temporarily unavailable by using physical or technical means. Data destruction can come from both cost considerations of the enterprise and external compliance or business requirements. Especially, if there are relevant data retention regulations, it should be considered that service providers should erase or anonymize collected data appropriately so that the data which has reached its retention limit or for which users have no longer given consent cannot be recovered.

– **Data backup and restoration**: The process of copying all or part of the data to other storage media to prevent data loss and to recover the original data with the backup data in case of data loss.

6.2 Threat analysis

Data in V2X communication also faces similar security threats and challenges to those defined in [ITU-T X.1603] and [ITU-T X.1641]. Some of these security threats and challenges for data in V2X communication include but are not limited to those presented in Table 6-1.

Table 6-1 – Threats and challenges according to data lifecycle in V2X communication

Data lifecycle	Security threats and challenges
Data collection	a) Data collection without authorization b) Acquisition interface vulnerabilities c) Spoofing d) Tampering and interception e) Insecure service access f) Unauthorized administrative access
Data transmission	a) Interception b) Masquerade c) Eavesdropping d) Unauthorized access e) Denial of service (DoS) attack
Data storage	a) Data loss and leakage b) Service unavailability
Data usage	a) Data misuse b) Insider threats c) System vulnerabilities d) Eavesdropping
Data migration	a) Data misuse b) System vulnerabilities c) Misrepresentation d) DoS attack
Data destruction	a) Spoofing b) System vulnerabilities
Data backup and restoration	a) System vulnerabilities

7 Categorized data in V2X communications

This clause provides the categorization policy for data handled by the V2X communication. The six data categories: object attribute data, vehicle status data, environmental perception data, vehicle control data, application service data, and user personal data are described in clause 7.2.

7.1 Data identification based on V2X communication scenarios

Data handled by the V2X communication can be identified based on an actual communication scenario. [ITU-T X.1372] categorizes the V2X communication scenarios as follows: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-nomadic device (V2D), and vehicle-to-pedestrian (V2P). This clause describes the relevant communication processes and data of each communication scenario.

7.1.1 Data in V2V communication

[ITU-T X.1372] identifies three V2V communication scenarios; V2V warning propagation, V2V platoon communication and V2V beaconing. In a V2V warning propagation scenario, a warning message is propagated between vehicles. In a V2V platoon communication scenario, groups of vehicles exchange vehicle status with each other. In a V2V beaconing scenario, each vehicle sends its vehicle status information. Table 7-1 shows data in V2V communication.

Table 7-1 – Data in V2V communication

Category	Scenario	Data
Vehicle-to-vehicle	V2V warning propagation	• Warning message • Basic safety message (BSM) • Cooperative awareness message (CAM)
	V2V platoon communication	• BSM • CAM
	V2V beaconing	• BSM • CAM

Technical specifications of BSM and CAM are described in [b-SAE J2735] and [b-ETSI TS 102 637-2] respectively.

7.1.2 Data in V2I communication

[ITU-T X.1372] identified two V2I communication scenarios; V2I warning and V2I information exchange. The V2I warning scenario allows exchanging of warning messages between a vehicle and infrastructures. In V2I information exchange, a vehicle and infrastructure communicate with each other to update traffic information and/or information regarding infotainment services. Table 7-2 shows data in V2I communication.

Table 7-2 – Data in V2I communication

Category	Scenario	Data
Vehicle-to-infrastructure	V2I warning	• Warning message
	V2I information exchange	• In-vehicle-signage • In-vehicle-information • Signal phase • Time of traffic light information • Road-surface condition • Weather condition • Visible-distance condition • Road construction information

7.1.3 Data in V2D communication

In a V2D communication scenario, a vehicle communicates with nomadic devices such as a smartphone, laptop and navigation system in the vehicle. [ITU-T X.1372] identifies two V2D communication scenarios; V2D communication by indirect links and V2D communication by direct links. The difference between these scenarios is the way of communication, and both handle the same types of data. V2P communication is considered as a specific case of V2D communication in [ITU-T X.1372]. Table 7-3 shows data in V2D communication.

Table 7-3 – Data in V2D communication

Category	Scenario	Data
Vehicle-to-nomadic device	V2D communication by indirect/direct links	• Vehicle hardware data • Vehicle software data • Device hardware data • Device software data • Service platform data • Application service data

7.2 Data categorization

This clause describes data categorization regarding data handled in V2X communication.

The data in V2X communication is taken into account to meet the related laws and regulations for personal data protection such as the general data protection regulation (GDPR), and the data described in this Recommendation cannot point to information of a specific or identifiable person.

7.2.1 Object attribute data

Object attribute data refers to the attributes of the entities in V2X communication, which can be subdivided into three types, that is, the attributes of vehicles, mobile devices and cloud service platforms:

– The attributes of vehicles data are related to the property of vehicles, such as brand, type, logo, colour.

– The attributes of a mobile device's data refer to the property related to the mobile device, such as the brand, type, colour.

– The attributes of service platform data are the property related to the service platform, such as the revision, manufacture and so on.

7.2.2 Vehicle status data

Vehicle status data refers to the status of vehicles which is closely related to the information service in V2X communication. It includes the operating states and parameters of these systems, such as the automotive powertrain system, chassis system, automotive safety system, body system, vehicle comfort system, and automotive electrical system.

More specifically, vehicle status data includes data information from the vehicle controller (such as pump control signal, air pressure sensor alarm, motor brake wired signal, etc.), transmitter system (such as torque, fuel consumption rate, etc.), cooling system (such as coolant temperature), gearbox system (such as the data of vehicle start, acceleration and acceleration, etc.), safety system (such as airbag status, seat belt usage status, etc.), chassis system (such as data information reflecting the status of vehicle network, steering system, ABS braking, tyre pressure monitoring, etc.), comfort system (such as data of air-conditioning opening, seat adjustment, window system, lighting use, etc.) and the other auxiliary systems.

Based on the description of vehicle running states, vehicle status data can be divided into two types, dynamic status data of vehicles and static status data of vehicles.

– Dynamic vehicle status data is related to the running states of the vehicle systems. Take the state of the air conditioning system as an example which depends on the temperature and humidity in the car.

- Static vehicle status data is related to the static status states of the air conditioning systems, such as seat belt usage status and status of air-conditioning, etc.

7.2.3 Environmental perception data

Environmental perception data is mainly related to the external environment of vehicles, including data information of the external equipment, terminals, pedestrians related to vehicle communication or interactions of information services in V2X communication, including but not limited to speed, traffic light information and road infrastructure in vehicle-vehicle communication. The information gathered by speed radars and cameras related to road infrastructure, the direction of driving and moving, the state of driving and moving, the speed, distance, the possible related state data of collision or not, and the data related to charging stations (piles) and other equipment acquired for electric vehicles are also elements of environmental data.

7.2.4 Vehicle control data

Vehicle control data is related to the control of the vehicle in V2X communication and mainly includes three subtypes, vehicle control data for auto-driving/intelligent assistant driving, remote operation and remote driving:

- Vehicle control data for auto-driving/intelligent assistant driving is the data of control instructions related to auto-driving or intelligent assistant driving. The data is based on the processing of the environment perception and intelligent decision-making systems and are used to realize the data for intelligent control behaviour of vehicles, such as brake or drive by wire, automatic gear shifting and integrated chassis control.
- Vehicle control data for remote operation refers to the instructions to vehicles through apps, service platforms, etc. and the data includes the data on remote door lock/unlock, remote control air-conditioning, remote windows operations and lights, etc.
- Vehicle control data for remote driving where the remote drive use-case is subdivided into several sub cases by distinguishing a human as a remote driver or a "cloud" as a possible remote driver. Vehicle control data for remote driving refers on outside-vehicle video streams showing the lane situations around a vehicle or outside-vehicle audio streams delivered to a remote driver as support of its decisions. In addition, data for remote driving can refer to an inside-vehicle video stream or an inside-vehicle audio stream delivered to a remote driver for monitoring situations. Furthermore, vehicle control data for remote driving refers to data on remote control instructions from the remote driver to the vehicle for e.g., accelerate or manoeuvre instructions, might be generated and sent when triggered by a control event, such as a brake instruction [b-ETSI TR 126 985], [b-3GPP TR 22.886].

7.2.5 Application service data

Application service data is related to the application of information interaction in V2X communication. It refers to the data related to information services in V2X communication besides object attribute data, vehicle status data, environmental perception data, vehicle control data and user personal data, including but not limited to information and entertainment data, traffic safety management and control data, and vehicle-related service data, etc.:

- Information and entertainment data is related to entertainment services provided in V2X communications, such as the multimedia download, website browsing and broadcast subscription of a certain population, as well as weather forecast, etc.
- Traffic safety management and control data are related to traffic safety and traffic management, such as road traffic safety early warning, emergency rescue, vehicle remote monitoring and management, etc.
- Vehicle-related service data is related to after-market services in V2X communication such as vehicle maintenance, second-hand vehicle management, financial insurance and related e-

commerce. For example, the maintenance frequency of certain types of automobile parts under a certain automobile brand belongs to vehicle-related service data.

7.2.6 User personal data

User personal data refers to the personal information concerning the user, which is used and/or generated in the V2X communication. This clause does not discuss the classification and protection of user personal data.

Therefore, if the data listed in Table 7-4 as an example corresponds to the user personal data in privacy related laws and in regulations such as the GDPR, then the categorization policy is overridden by that regulation.

7.3 Data security levels

Based on the consideration combined with the data security objectives, the importance of the data, and the impact of the possible security events, each data category can be classified into 3 levels:

- **Level 1** (less protected data) contains data that is publicly available data in V2X communications such as the software version of the V2X platform.
- **Level 2** (moderately protected data) contains data that is required to be protected with security measures, such as the vehicle data acquired in V2V communication, login account and password of V2X communication.
- **Level 3** (highly protected data) contains data that is required to be more strongly protected than Level 2 (moderately protected data) in V2X communications, such as the financial transaction information in V2D communication, key performance data of a vehicle and identity authentication information of V2X communications.

Confidential data only refers to the confidential data from enterprises related to V2X communication, and the user's personal information is not involved here.

Table 7-4 provides detailed information on data security levels and examples in V2X communications.

Table 7-4 – Examples of data security levels in V2X communication

Data category in V2X communications		Data security level in V2X communications	Examples
Object attribute data	Attribute data of vehicle	Level 1	The brand, type, logo, colour of a vehicle.
		Level 2	Performance parameters of a certain type of vehicle.
		Level 3	Specific hardware and software configuration data of a certain type of vehicle.
	Attribute data of mobile device	Level 1	The brand, type, logo, colour of a mobile terminal.
		Level 2	Equipment status data related to some important functions in V2X communication.
		Level 3	The critical performance parameters and configuration information of a type of mobile device.
	Attribute data of cloud service platform	Level 1	The type and name of a cloud service platform.
		Level 2	The information of hardware, operating system or application software.
		Level 3	The critical performance parameters and configuration information of a service platform.

Table 7-4 – Examples of data security levels in V2X communication

Data category in V2X communications		Data security level in V2X communications	Examples
Vehicle status data	Dynamic vehicle status data	Level 1	The state of an air-conditioning system. Inside temperature of vehicles.
		Level 2	Running state of an airbag and air belts, etc. Data perceived by sensors within a vehicle and closely related to important vehicle handling, such as tire pressure.
		Level 3	Core running technical indicators of a vehicle Data received by sensors within a vehicle and closely related to critical vehicle handling, such as data from collision sensors.
	Static vehicle status data	Level 1	The frequency of use of an air-conditioning system in a certain time.
		Level 2	Average fuel consumption of a vehicle.
		Level 3	The confidential data of the vehicle system.
Environmental perception data	Vehicle external environmental perception data	Level 1	Road type (expressway or country road or sidewalk), road condition (intact or wet or slippery), road speed limit, distribution and status information of signal lights, status information of signal lights, road congestion, traffic accidents, etc.
		Level 2	In the vehicle-vehicle communication scenario, the information after desensitization of nearby vehicles, such as the physical location, longitude and latitude, update time, driving speed, forward direction, lane change information. In the vehicle-pedestrian communication scenario, the data after desensitization such as the location, distance, speed and motion state of the approaching pedestrians, and the possibility of collision.
		Level 3	In vehicle-vehicle communication scenarios, data information of adjacent vehicles in a certain period of time after desensitization, such as travel route, location, time, parking information, etc.
Vehicle control data	Vehicle control data for auto-driving/intelligent assistant driving	Level 1	Sound data for backing tips in backing assistance.
		Level 2	In the lane-keeping application of the intelligent assistant driving system, when the vehicle tends to deviate from the driving lane, the warning command data such as steering wheel jitter, dashboard red light or green light indication are sent.
		Level 3	The confirmation instructions of Intelligent Parking System in automatic parking.
		Level 1	General reading data related to remote monitoring of V2X communication

Table 7-4 – Examples of data security levels in V2X communication

Data category in V2X communications		Data security level in V2X communications	Examples
	Vehicle control data for remote operation	Level 2	Instruction to remote start the vehicle or start up the steering of vehicles.
		Level 3	Implementing instructions related to remote control of multiple vehicles, such as fleet, through the service platform of V2X communications.
	Vehicle control data for remote driving	Level 1	An inside-vehicle video stream and an inside-vehicle audio stream whose delay requirements can be more relaxed than those of outside-vehicle video and audio, may be used by the remote driver to monitor the status of the inside vehicle.
		Level 2	Outside-vehicle audio streams may be delivered to a remote driver for conveying the noises and horn sounds from other vehicles.
		Level 3	Sensors or rendering devices such as display or sound system are used for manoeuvre instructions from the remote driver. Instructions should be provided with high reliably and at low latency and needs to be acknowledged especially in relation to alarm event (e.g., brake instruction). The video (camera) and audio (microphone) sensor data (maybe also radar or lidar sensor data) recording external sounds or videos for early and non-visual identification of obstacles in the route such as emergency vehicles, pedestrians, etc. Vehicle status sensor (Acceleration, Speed, direction, Position, etc.) data may be sent with a fixed interval from vehicle to remote driver with high reliability because some sensor streams might be essential for the correct driving operations.
Application service data	Information and entertainment data	Level 1	Data of radio broadcast
		Level 2	Browsing records of online shopping after desensitization
		Level 3	Speech and video recordings after desensitization in information service applications
	Traffic safety management and control data	Level 1	Road traffic congestion warning, real-time traffic accident warning data, etc.
		Level 2	Vehicle collision warning data due to vehicle parking in front of vehicle in queue
		Level 3	Remote monitoring data of road traffic vehicles.
	Vehicle-related service data	Level 1	After desensitization, the usage behaviour data of the entertainment system related to the use, operation and other information of the vehicle entertainment system are recorded.

Table 7-4 – Examples of data security levels in V2X communication

Data category in V2X communications		Data security level in V2X communications	Examples
		Level 2	After desensitization, the vehicle behaviour data related to the vehicle driving behaviour.
		Level 3	Data after desensitization, such as car owner's personal preferences and behaviour habits based on vehicle travel time, route, location, and information and entertainment system's use behaviour data, or core vehicle parameters based on vehicle's own state and environment perception data, etc.
User personal data	N/A	N/A	N/A

The contents of Table 7-4 are described as follows:

1) N/A: not applicable
2) The data after desensitization described in Table 7-4 cannot directly or indirectly identify or indicate the personal information of persons, after being processed by anonymous fuzzy and other technical means. Data desensitization methods include but are not limited to anonymity, de-identification, diversity, data suppression, data disturbance, differential privacy, etc. The organization related to V2X communication should take appropriate data desensitization measures based on the comprehensive consideration of data subject characteristics, data sensitivity level, and data operation requirements.

8 Security requirements

This clause provides the basic security requirements, intermediate security requirements and advanced security requirements which strictly correspond to level 1-3 data.

8.1 Security requirement level

Based on the classification for categorized data, security methods or measures for each level are stated. There are three security levels of security requirements that can be adopted: the basic security requirements, the intermediate security requirements and the advanced security requirements. Generally, the basic security requirements are taken to protect level 1 (less protected data), the intermediate security requirements are taken to protect level 2 (moderately protected data), and the advanced security requirements are taken to protect level 3 (highly protected data). Table 8-1 describes security requirements according to security level of V2X communication data.

Enterprises can also choose the security measures according to their own situation or the confidentiality of the data.

Table 8-1 – Security requirements according to security level of V2X communication data

Security level of V2X communication data	Level of security requirements		
	Basic	Intermediate	Advanced
Level 1 (less protected data)	*	N/A	N/A
Level 2 (moderately protected data)	*	*	N/A
Level 3 (highly protected data)	*	*	*
*: Covered; N/A: Not applicable.			

8.2 Basic security requirements

(1) Data collection

- Data in V2X communications should be classified according to the combination of the data security objectives, the importance of the data and the impact of the possible security events.
- The principle of minimization should be followed in the process of data collection. Only data related to business functions can be collected.
- The collected data should be classified and managed according to the data classification and classification methods described in clause 6 and clause 7. Different security measures should be formulated and implemented for different levels of data.

(2) Data transmission

- The overall security requirement of data transmission in V2X communications should not be lower than that of general communication network.
- According to different data categorizations, business processes and security risks of V2X communication scenarios, different data transmission security strategies and measures should be adopted.
- Security protocols such as transport layer security (TLS) should be used to ensure the security of data transmission in the communication scenarios between the vehicle and other entities.
- Should be able to detect that the data was corrupted during transmission.

(3) Data storage

- For data stored in the vehicle terminals and service platforms, data encryption mechanisms should be adopted in the V2X communication related equipment and systems. The parameters such as the algorithm, strength, and mode of cryptography should be supported by an optional configuration.
- It should be able to ensure the security of cache data in the service platform or vehicle system. It should encrypt the data stored in the cache system.
- For data stored in the vehicle terminals and service platforms, data access control mechanisms should be adopted to prevent unauthorized access, modification and deletion, and cross-domain information access.
- It should be able to verify the integrity of the data in the storage process to prevent data from being tampered with, deleted and inserted. User warning information should be provided when the integrity of data is destroyed.

(4) Data usage

- The data should be processed within the scope of authorization, limited to the minimum range of business needs.
- The use of data should be authorized and verified.
- The purpose and scope of data usage should meet the requirements of relevant national laws and regulations.
- During data analysis and mining, the source data and mining results should be signed to prevent data from being maliciously deleted, tampered with, or unrestricted abuse.
- For the data transfer or export between the Internet of vehicles devices, systems and platforms, management and technical measures should be adopted to ensure security.

(5) Data migration

- Security capability assessment should be conducted before data migration to ensure the safety of data migration.
- The continuity of business and application should be ensured when data is migrated between different data devices.
- It should establish a migration scheme, assess its feasibility and associated risks, then develop risk control measures accordingly as preparations for data migration.

(6) Data destruction

- A data destruction strategy and management system should be established to clarify the object and process of destruction. The examination and approval mechanism for data destruction should be established, and the relevant supervisory role for destruction should be set up to supervise the destruction process.
- Measures should be provided to clear the data which has reached its retention limit, or when users no longer give consent, the data should be destroyed immediately.
- Measures should be provided to help clear the data left over from data migration or business.
- Measures should be provided to remove all copies of backup data.

(7) Data backup and restoration

- Data backup and recovery mechanisms should be established before data migration.
- Local data backup and recovery should be provided.
- A regular full data backup mechanism should be established, and the recommended time cycle should not be less than once a week.
- The backup data should have the same access control rights and secure storage requirements as the original data.

8.3 Intermediate security requirements

The intermediate security requirements is a set of supersets of the basic security requirements. Based on requirements of the basic security requirements in each data lifecycle phase, the following requirements are added:

(1) Data collection

In addition to meeting basic security requirements, the following requirements should also be met:

- During the collection of level 2 data, the original data should be backed up to avoid data omission and loss.
- Identification mechanisms should be adopted to ensure the authenticity of data collection.

- Data verification mechanisms should be adopted to ensure the integrity of data collection.

(2) Data transmission

In addition to meeting basic security requirements, the following requirements should also be met:

- The data transmission of the core service platform of automobile and Internet of vehicles should adopt private network or virtual private network communication to realize isolation from Internet.
- In V2V/V2I communication, it should have a trusted identity certificate, which can verify the identity of the data transmission node, and the authentication information should not disclose privacy information.
- The vehicle should be able to identify the illegal connection requests from cellular networks to filter malicious packets.
- For level 2 data, such as remote control instruction data, the reliability of the data source should be verified to ensure that the data is not forged.

(3) Data storage

In addition to meeting basic security requirements, the following requirements should also be met:

- It should be able to verify the integrity of the data in the storage process to prevent data from being tampered with, deleted and inserted, and necessary restoration measures should be provided when the integrity of data is destroyed.
- The identification information should be set for the data files stored in the intelligent connected vehicle (ICV), service platforms and applications to avoid the use of such files in unauthorized devices and systems.
- For the caching system of the service platform in V2X communication, specific operational records should be kept to protect the cashed level 2 data.
- The whole process of data log management should be established to prevent data repudiation threats.

(4) Data usage

In addition to meeting basic security requirements, the following requirements should also be met:

- For a data query of level 2 data, the operations, such as query, external display and statistics, fuzzy processing should be carried out.
- The usage of level 2 data should be audited and an audit log should be generated.

(5) Data migration

In addition to meeting basic security requirements, the following requirements should also be met:

- The migration plan should be developed, its feasibility and related risks should be evaluated, and then the corresponding risk control measures should be formulated to prepare for data migration.

(6) Data destruction

In addition to meeting basic security requirements, the following requirements should also be met:

- It should be ensured that the storage space of resources related to V2X communication, such as files, directories and database records, is not released or reallocated to other users until these resources are completely cleared.

- For the on-board terminal, in order to prevent data leakage due to replacement of vehicle components, it should be able to provide the function of erasing the data of vehicle terminal, so as to ensure that the erased data of the vehicle terminal cannot be recovered.

(7) Data backup and restoration

In addition to meeting basic security requirements, the following requirements should also be met:

- For local or remote backup data, full data should be backed up at least once a week, and incremental backups should be backed up at least once a day. In addition, a multi backup mechanism should be established.
- Backup data should be encrypted and stored.

8.4 Advanced security requirements

The advanced security requirements is a set of supersets of the intermediate security requirements. Based on requirements of the intermediate security requirements in each data lifecycle phase, all the following requirements should be adopted.

(1) Data collection

- The protection requirements are the same as those of the intermediate security requirements.

(2) Data transmission

In addition to meeting the security requirements of the intermediate security requirements, the following requirements should also be met:

- It should be able to detect data integrity damage during transmission and take necessary measures to recover data when integrity damage is detected.
- For confidential data of L3 level, mutual authentication should be adopted to deal with the threat of tampering and data leakage caused by identity impersonation of external entities.

(3) Data storage

In addition to meeting the security requirements of the intermediate security requirements, the following requirements should also be met:

- The hardware security encryption storage scheme should be adopted to ensure the confidentiality of confidential data of vehicles, service platforms, intelligent mobile terminal applications and roadside infrastructure.
- It should be able to verify the integrity of the data in the storage process to prevent data from being tampered with, deleted, and inserted, and necessary restoration measures should be provided when the integrity of data is destroyed.

(4) Data usage

In addition to meeting the security requirements of the intermediate security requirements, the following requirements should also be met:

- The approval of secondary operation authority should be carried out by multi person authorization mode.
- Data correlation isolation should be conducted to prevent data leakage due to data association analysis for the data in different systems, platforms or applications.
- Dynamic desensitization should be supported in the use of confidential data.

(5) Data migration

The protection requirements are the same as those of the intermediate security requirements.

(6) Data destruction

In addition to meeting the security requirements of the intermediate security requirements, the following requirements should also be met:

- Should provide means to prevent the recovery of destroyed data.

(7) Data backup and restoration

In addition to meeting the security requirements of the intermediate security requirements, the following requirements should also be met:

- Security authentication measures, such as identity authentication, should be provided to ensure that local and remote data backup and recovery operations can only be performed with the knowledge or control of authorized users.

Bibliography

[b-ITU-T X.1217]	Recommendation ITU-T X.1217 (2021), *Guidelines for applying threat intelligence in telecommunication network operation*.
[b-ITU-T X.1751]	Recommendation ITU-T X.1751 (2020), *Security guidelines for big data lifecycle management by telecommunication operators*.
[b-3GPP TR 22.886]	3GPP TR 22.886 V16.2.0 (2018), *Study on enhancement of 3GPP Support for 5G V2X Services (Release 16).*
[b-ETSI TR 126 985]	ETSI TR 126 985 V16.0.0 (2020), *5G Vehicle-to-everything (V2X) Media handling and interaction (3GPP TR 26.985 version 16.0.0 Release 16).*
[b-ETSI TS 102 637-2]	ETSI TS 102 637-2 (2011), *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*.
[b-SAE J2735]	*V2X Communications Message Set Dictionary,* (July 2020).

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

Published in Switzerland
Geneva, 2023