Security Guideline

for

Driver Assistance Communications System

ITS FORUM RC-009 Ver. 1.1

Established on April 27, 2011

Updated on April 25, 2012

ITS Info-communications Forum

of Japan

Security Guideline

for

Driver Assistance Communications System

ITS FORUM RC-009 Ver. 1.1

Established on April 27, 2011

Updated on April 25, 2012

ITS Info-communications Forum

of Japan

Revision History

Ver.	Date	Chapter/Section	Reason	Revised Content
1.0	April 27, 2011	Establishment	Newly established	
1.1	April 25, 2012	Annex D	TG assessment content added	Consider primitives for storing/updating/ changing security information

[Blank]

Security Guideline for Driver Assistance Communications System

Table of Contents

Chapter 1: Outline of Operation Model and Application Scope

1.1 Purpose

This guideline, having the safety of vehicles and occupants as a first priority, describes measures to be implemented for ensuring the security of inter-vehicle and roadside-to-vehicle communication information in a driver assistance communications system, with the aim of maintaining the intended performance for all vehicles and the system itself.

The guideline covers the security aspect of services and content management as described in the Operation Management Guideline [1].

The basic policies are as follows:

- Protect information resources from threats related to information communication, in order to maintain the quality of provided services. If an attack has temporarily disabled protection, provide measures to quickly restore protection.
- If the driver assistance service is elevated to a level beyond the currently envisioned level, elevating security to match the service characteristics beyond the measures described here must also be considered.
- Depending on the characteristics of the provided service, the handled information resources may be critical for human life and safety. Protection of information resources is of course important, but in devising information security measures to guard against possible attacks, failsafe measures must also be implemented.
- Information related to the legal regulations compliance of provided services must also be protected.

1.2 Operation management model

The main entities involved in operation of the driver assistance communications system and their respective relationships are outlined in the diagram below.

(1) Entities and their relationship

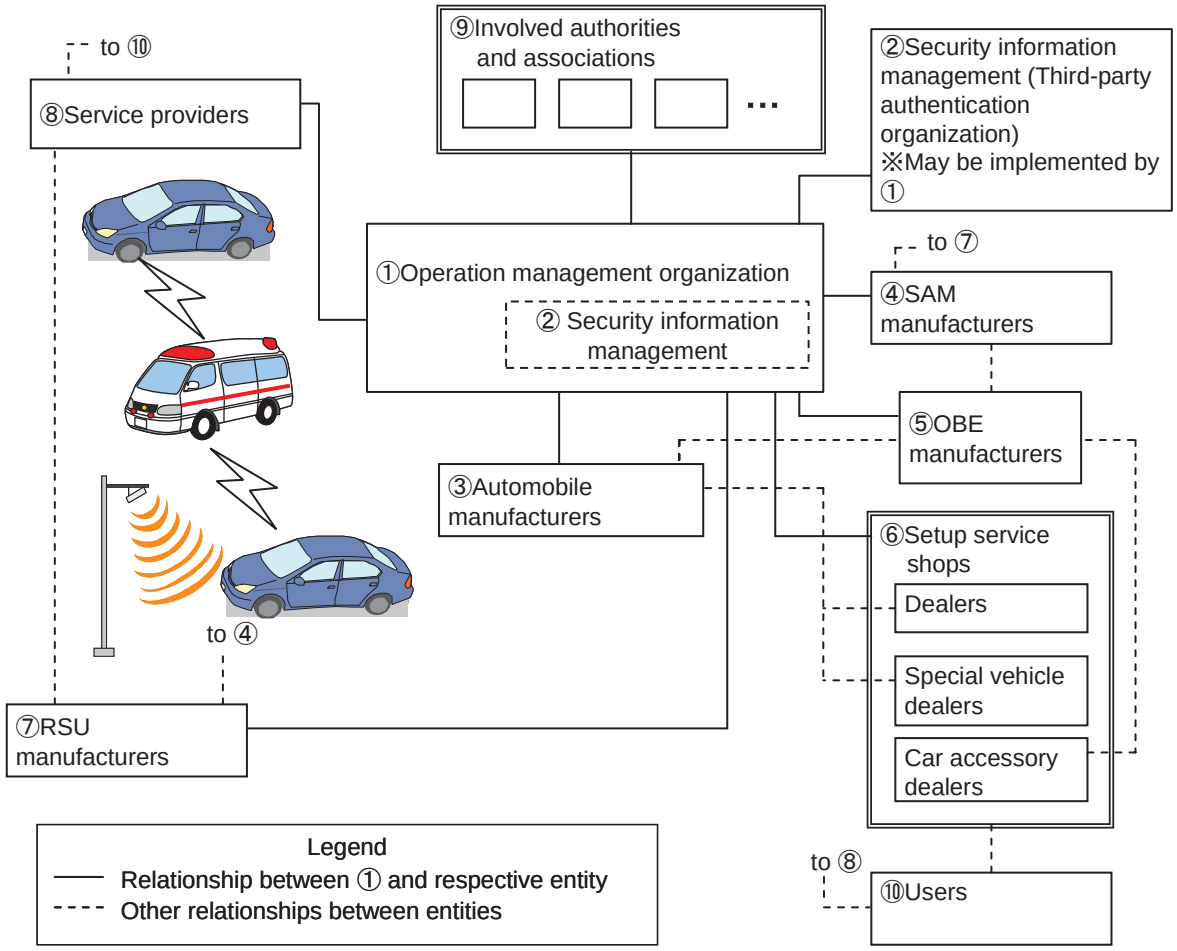


Figure1-1: Operation management organization and other entities

(2) Role of each entity

The proposed major roles of each entity are listed below. The names used for the entities are for convenience and express their function. A single enterprise or organization may fulfill the roles of several entities.

Table 1-1: Role of each entity

Entity	Role
① Operation management organization	・Management of RSUs, OBE and other hardware ・Radio management within system and with regard to other systems ・Management of roadside-to-vehicle communications and inter-vehicle communications ・Management of system security and other services and content aspects ・User support, system promotion activities, and other tasks
② Security information management (may be implemented by operation management organization)	・Authentication of RSUs and OBE
③ Automobile manufacturer	・Manufacture and marketing of vehicles with OBE
④ SAM manufacturer	・Development and manufacture of SAM for RSUs and OBE
⑤ OBE manufacturer	・Manufacture and marketing of OBE
⑥ Setup service shop (dealer, special vehicle dealer, car accessory dealer)	・Set up equipment and store the necessary information for operation (emergency vehicles at special vehicle dealers only)
⑦ RSU manufacturer	・Manufacture and marketing of RSUs
⑧ Service provider	・OBE user management ・Provide information distribution services and other services for driver assistance in inter-vehicle communication (if only inter-vehicle communication services are being provided) ・Provide information collection and distribution services and other services for driver assistance in roadside-to-vehicle communication ・Ownership of RSUs ・Operation checking of RSUs
⑨ Involved authorities and associations	・Accreditation, linking to other safety related systems, etc.
⑩ Users	・Benefit from services

(3) Entity registration and management

The operation management organization must perform registration of entities such as service providers, manufacturers, setup service shops, and dealers that were contracted for the service, in order to ensure proper entity management. Besides implementing the registration function, the operation management organization must establish an operation framework and define entity management regulations that clearly describe and define the roles, rights, and obligations of registered entities.

1.3 Application scope

Among the functions of the operation management organization, this guideline covers the scope shown in Figure 1-2 below:

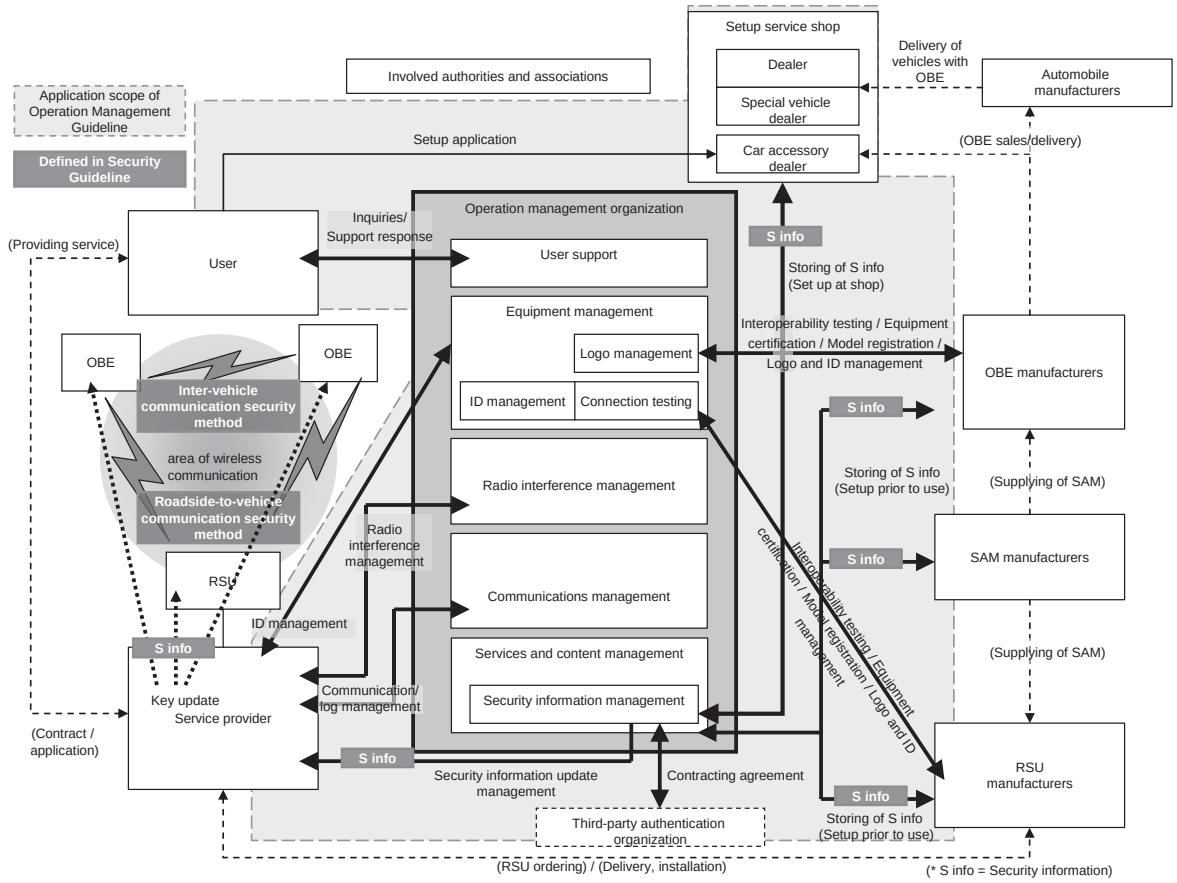


Figure1-2 Application scope of Operation Management Guideline

The role of the operation management organization comprises the following functions:

< Equipment management >

- Provide an environment for RSU and OBE interconnectivity testing
- Perform RSU and OBE interconnectivity testing and certify equipment compatibility
- Perform RSU and OBE model registration and logo use management
- Perform RSU and OBE ID management
- Manage normal operation of RSU and OBE during use

＜Radio management＞

- Perform radio interference management (prevent and manage interference with systems using adjacent frequency bands, other driving safety related systems, etc.)

- Liaise with other systems (conclude agreements for example on cost distribution for interference prevention with adjacent frequency systems and other driving safety related systems, etc.)
- Manage normal operation of the radio (while system is operating)

＜Communications management＞

- Management of normal communications operation
- Manage communication logs

＜Services and content management＞

- Provide and maintain an environment that ensures system security
- Establish and operate a security related setup environment for equipment
- Security information update management
- Cancellation of security information

＜Other items＞

- Entity registration and management
- User support
- Establish and maintain a framework, promote acceptance and use of the system, etc.

1.4 Definition of terms

1.4.1 Terms

The terms used in this document are defined in Table 1-2.

Table1-2 Definition of terms

Term	Definition
OBE	Radio equipment that can directly and efficiently communicate with other vehicles or RSUs with the aim of providing driver assistance. Must have all or some of the following functions: ① Ability to exchange information with other equipment on board the vehicle ② Ability to detect the state of the current vehicle ③ Ability to alter the state of the current vehicle ④ Ability to provide information to the occupants of the current vehicle In particular, the term refers to OBE registered for the current system.
RSU	Stationary radio equipment installed at the roadside that uses detected information about traffic conditions (from roadside sensors or similar) and infrastructure information about traffic signal status, etc. to efficiently provide assistance to vehicles traveling within the communication area. In particular, the term refers to roadside equipment registered for the current system.
Third party	An outside party not owning OBE for the current system
User	A party owning OBE for the current system
Service personnel	A person providing maintenance for OBE, RSUs, or vehicles
Communication equipment	A communication device other than OBE or RSU
SAM	Short for Secure Application Module. A module storing information and using encryption or other means to make such information held within OBE secure and tamper-proof.
Negative list	A list of IDs and public key certificates of invalid equipment (OBE and RSUs). Includes CRL and expired equipment ID lists.
Security information	In order to enable secure exchange of data in inter-vehicle communication and roadside-to-vehicle communication, means such as keys, certificates, and digital signatures are used. These are globally referred to as security information. In the diagrams and tables of this document, the term is abbreviated as “S info.”

1.4.2 Abbreviations

AES	:	Advanced Encryption Standard
CA	:	Certificate Authority
CBC	:	Cipher Block Chaining
CCM	:	Counter with CBC-MAC
CRL	:	Certificate Revocation List
CRYPTREC	:	Cryptography Research and Evaluation Committees
CTR	:	Counter
DoS	:	Denial of Service
ECDSA	:	Elliptic Curve Digital Signature Algorithm
ETSI	:	European Telecommunications Standards Institute
GPS	:	Global Positioning System
MAC	:	Message Authentication Code
OCSP	:	Online Certificate Status Protocol
PKI	:	Public Key Infrastructure
SAM	:	Secure Application Module

1.5 Reference materials

[1] Operation Management Guideline for Driver Assistance Communications System

[2] C. Laurendeau and M. Barbeau, “Threats to Security in DSRC/WAVE,” ADHOC-NOW Lecture Notes in Computer Science, Volume 4104, 2006 page.266-279.

[3] Bryan Parno and Adrian Perrig, “Challenges in securing vehicular networks”, In Workshop on Hot Topics in Networks (HotNets-IV), 2005

[4] M. Raya, P. Papadimitratos and J-P. Hubaux, "Securing Vehicular Networks", IEEE Wireless Communications, Volume 13, Issue 5, October 2006

[5] M. Raya and J.-P. Hubaux, “Security Aspects of Inter-Vehicle Communications”, In Proceedings of STRC 2005 (Swiss Transport Research Conference), March 2005

[6] IPA, “Survey of Security in Embedded Systems in Vehicles and Digital Home Appliances,” March 2009

[7] M. Barbeau, “WiMax/802.16 threat analysis”, Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks (Q2SWinet),

2005

[8] IEEE 1609.2, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, 2006/7

[9] NIST Special Publication 800-38C, “Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality”

Chapter 2: Services Envisioned by This Guideline

2.1 Driving safety assistance service using inter-vehicle communication

Concrete examples of service scenarios envisioned by this guideline are shown below.

2.1.1 Prevention of collision when making a left turn

・Service outline

At an intersection, information about two-wheeled vehicles or similar approaching from the rear on the left is provided to the driver of a vehicle attempting to make a left turn.

・Service scenario

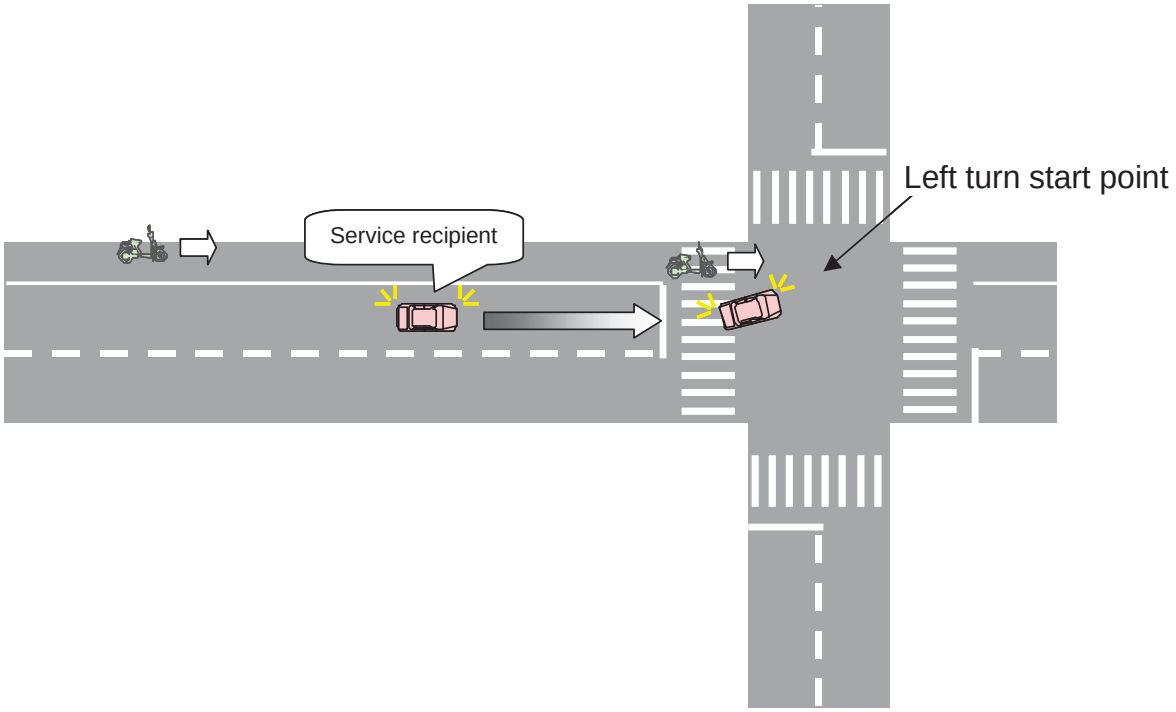


Figure 2-1: Service scenario for prevention of collision during left turn

2.1.2 Prevention of collision when making a right turn

・Service outline

At an intersection, information about oncoming vehicles or similar is provided to the driver of a vehicle waiting to make a right turn.

・Service scenario

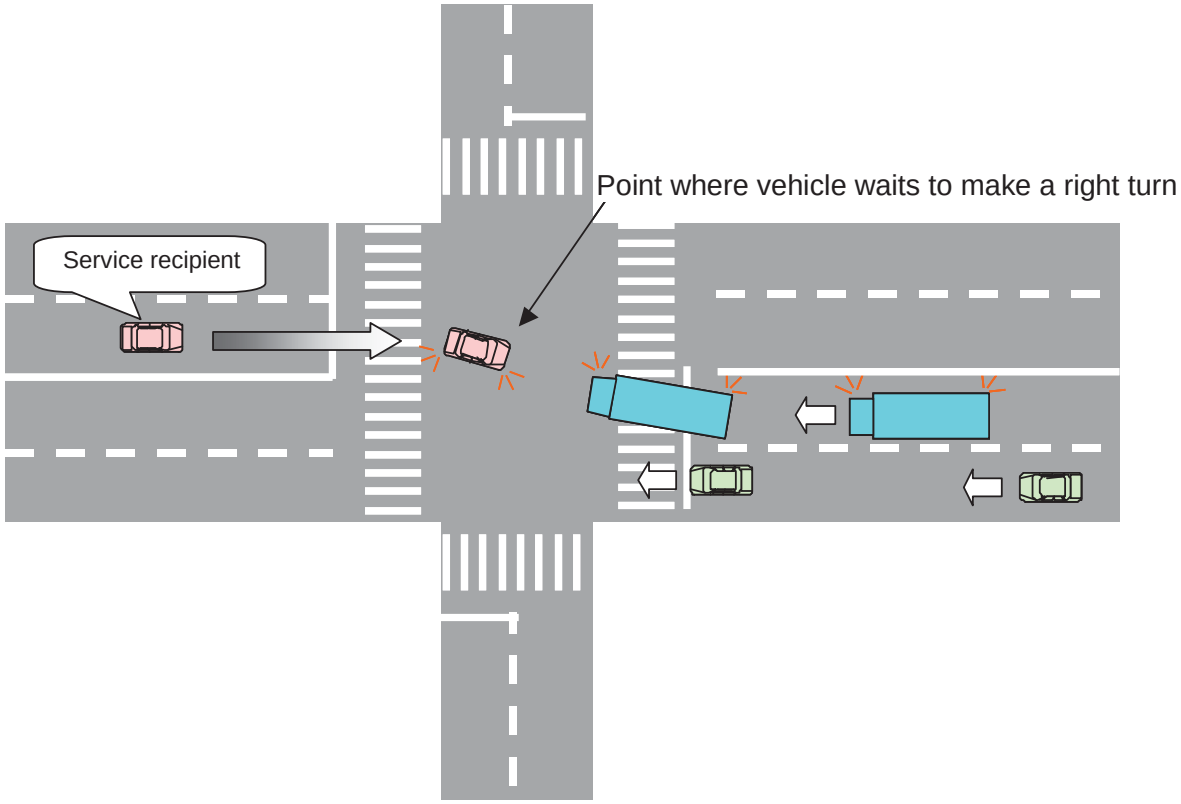


Figure 2-2: Service scenario for prevention of collision during right turn

2.1.3 Prevention of collision at intersection (no stop sign on either road, intersection in built-up area)

・Service outline

At an intersection without stop signs, information about vehicles in the intersecting road is provided to the driver of a vehicle approaching the intersection.

・Service scenario

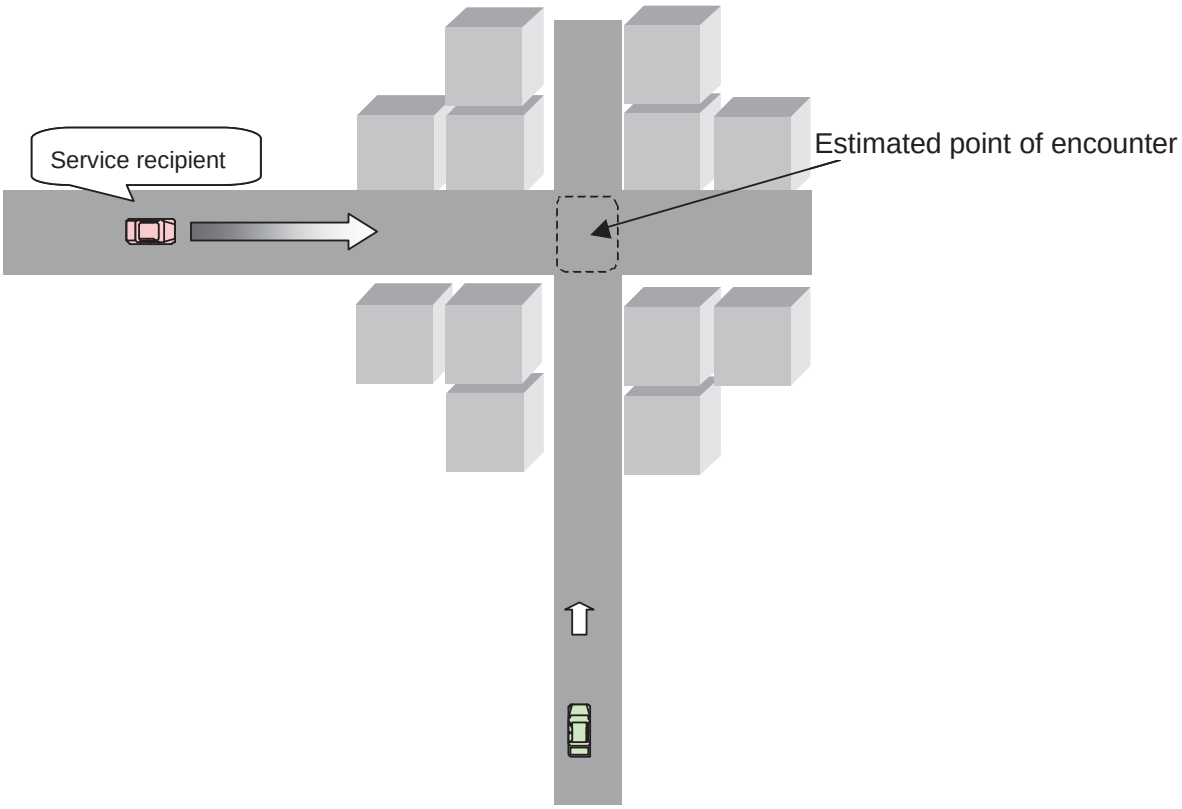


Figure 2-3: Service scenario for prevention of collision at intersection (no stop sign on either road, intersection in built-up area)

2.1.4 Prevention of collision at intersection (assistance for stopping, stop sign present, no line of sight)

・Service outline

At an intersection with a stop sign but no clear line of sight to the intersecting road, information about vehicles in the intersecting road is provided to the driver of a vehicle approaching the intersection.

・Service scenario

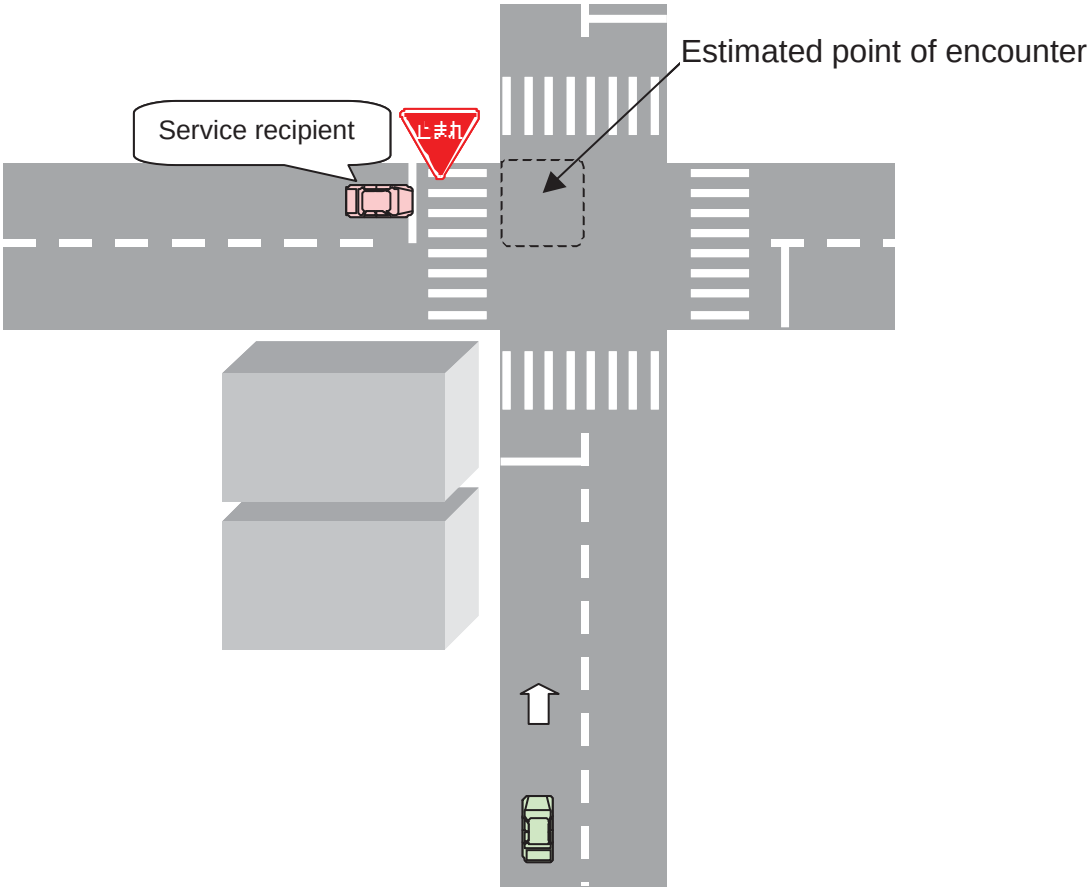


Figure 2-4: Service scenario for prevention of collision at intersection (stop sign present, no line of sight)

2.1.5 Prevention of rear end collision

・Service outline

At a location such as a curve with bad visibility, information about a slow or stopped vehicle ahead is provided to the driver of a vehicle following in the same lane.

・Service scenario

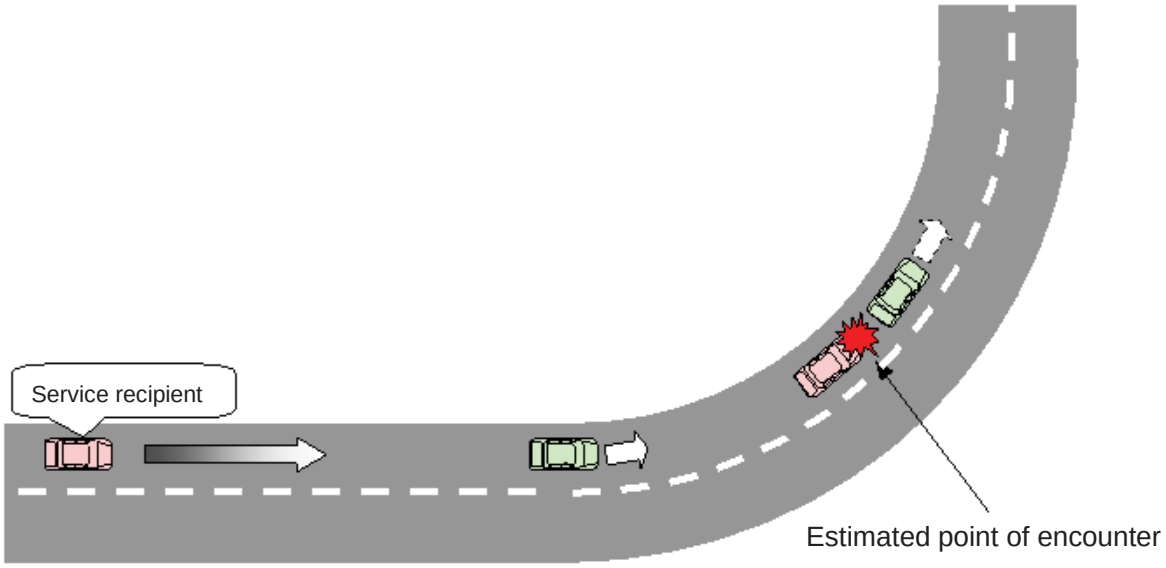


Figure 2-5: Service scenario for prevention of rear end collision

2.1.6 Provision of emergency vehicle information

・Service outline

Information about a vehicle on emergency duty is provided to drivers of vehicles in the vicinity.

・Service scenario

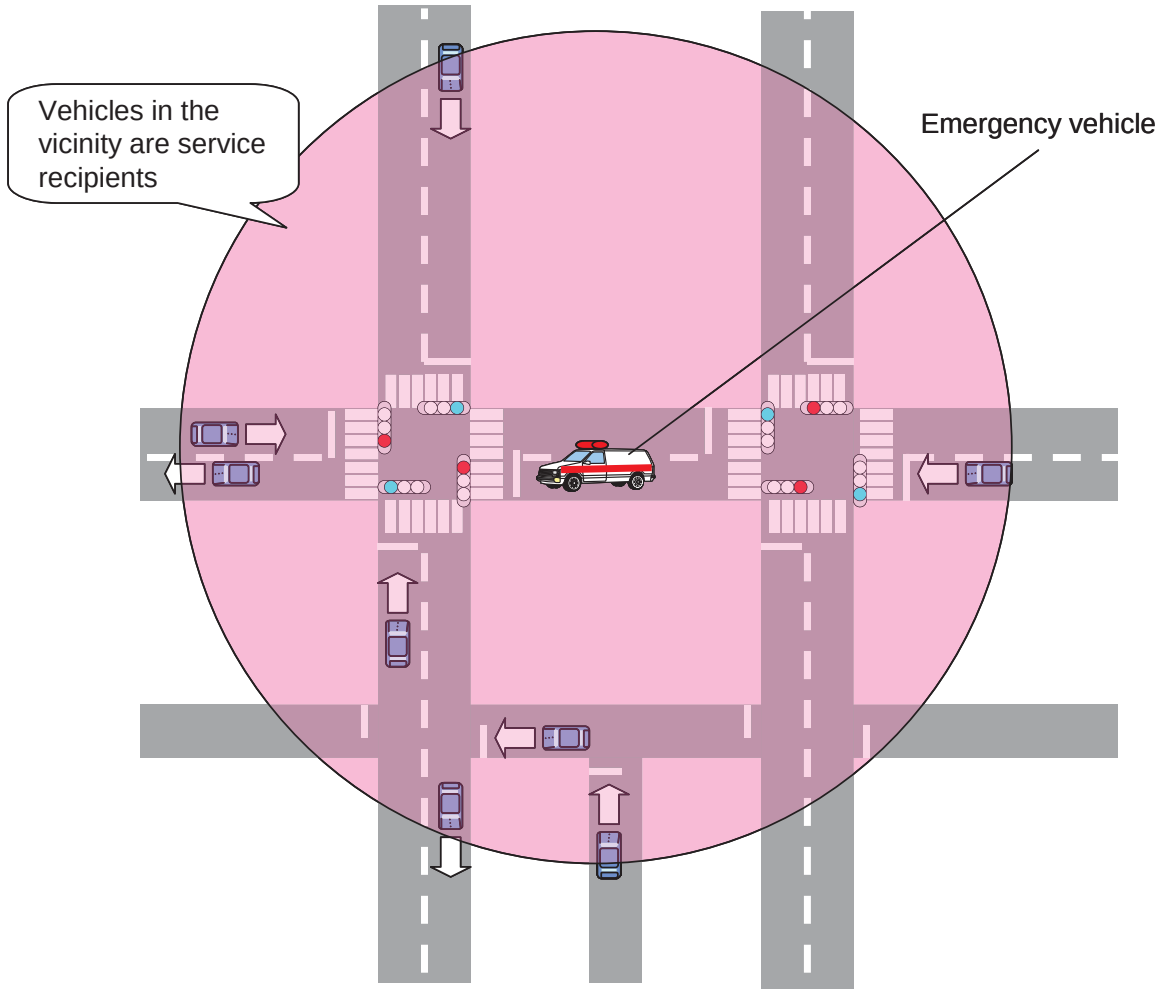


Figure 2-6: Service scenario for providing emergency vehicle information

2.2 Driving safety assistance service using roadside-to-vehicle communication

Concrete examples of service scenarios for roadside-to-vehicle communication envisioned by this guideline are shown below.

2.2.1 Prevention of collision at intersection

・Service outline

At an intersection without traffic signals, a roadside sensor or similar detects vehicles in the intersecting road, and the information is provided to the driver of a vehicle approaching the intersection.

・Service scenario

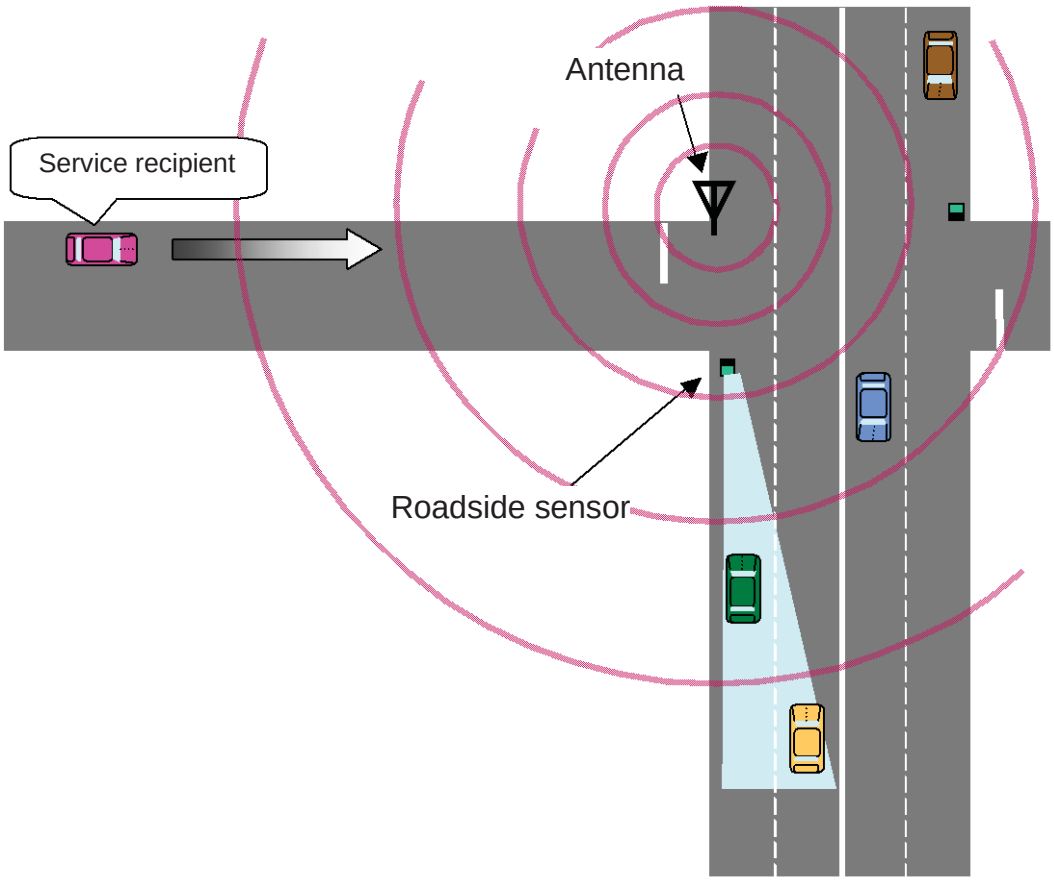


Figure 2-7: Service scenario for prevention of collision at intersection

2.2.2 Prevention of collision when making a right turn

・Service outline

At an intersection, a roadside sensor or similar detects oncoming vehicles or similar, and the information is provided to the driver of a vehicle attempting to make a right turn.

・Service scenario

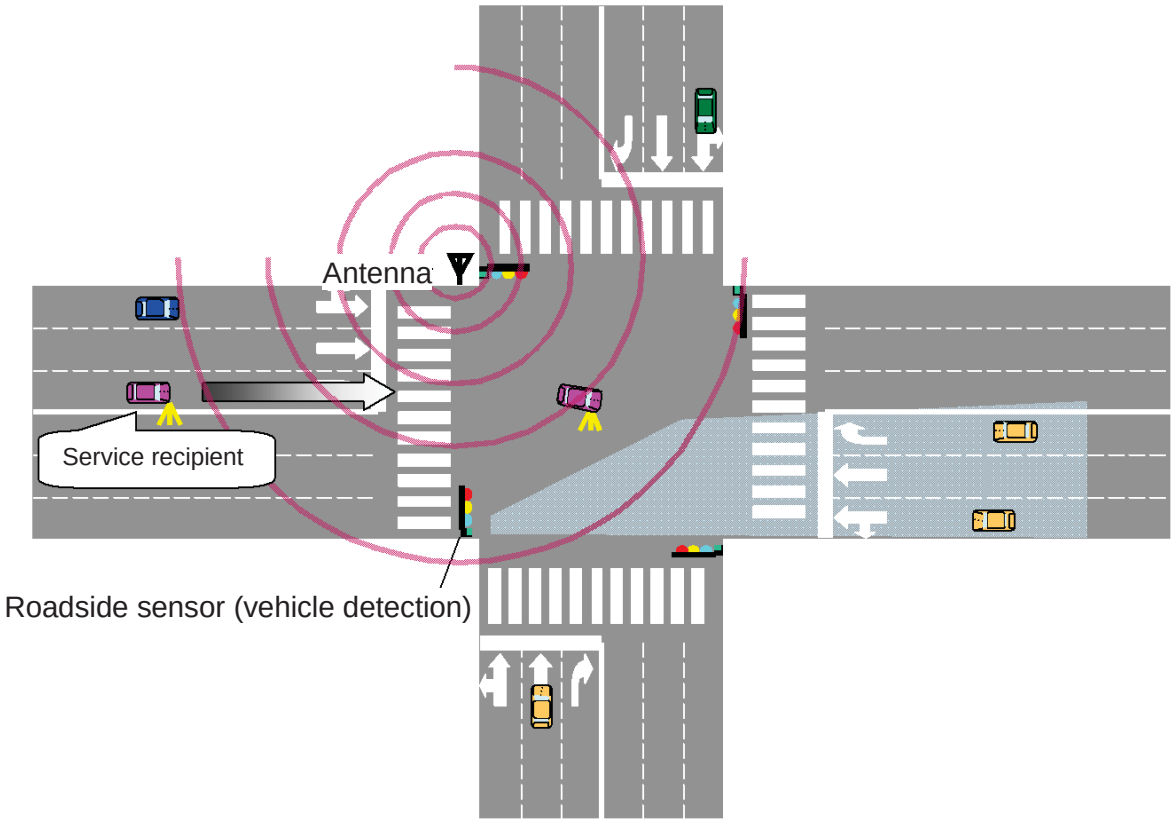


Figure 2-8: Service scenario for prevention of collision during right turn

2.2.3 Prevention of collision when making a left turn

・Service outline

At an intersection, a roadside sensor or similar detects two-wheeled vehicles or similar approaching from the rear on the left, and the information is provided to the driver of a vehicle attempting to make a left turn.

・Service scenario

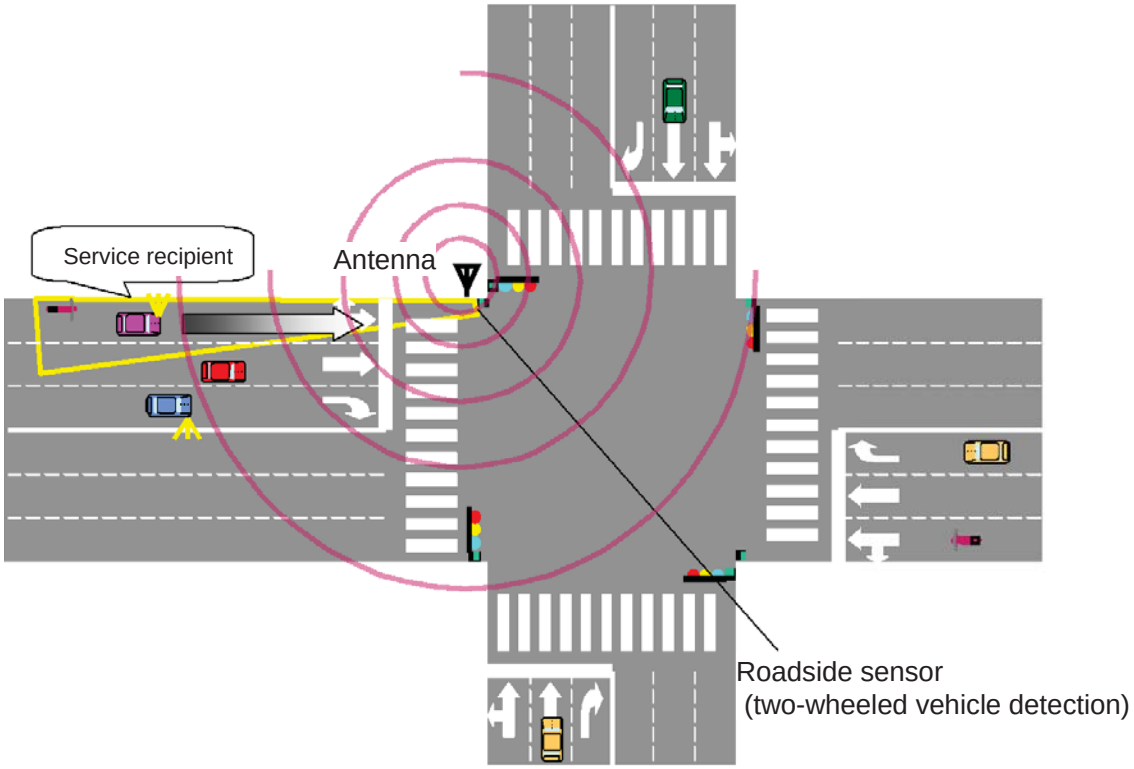


Figure 2-9: Service scenario for prevention of collision during left turn

2.2.4 Prevention of rear end collision

・Service outline

At a location such as a curve with bad visibility, a roadside sensor or similar detects the presence of vehicles ahead, and the information is provided to the driver of a vehicle following in the same lane.

・Service scenario

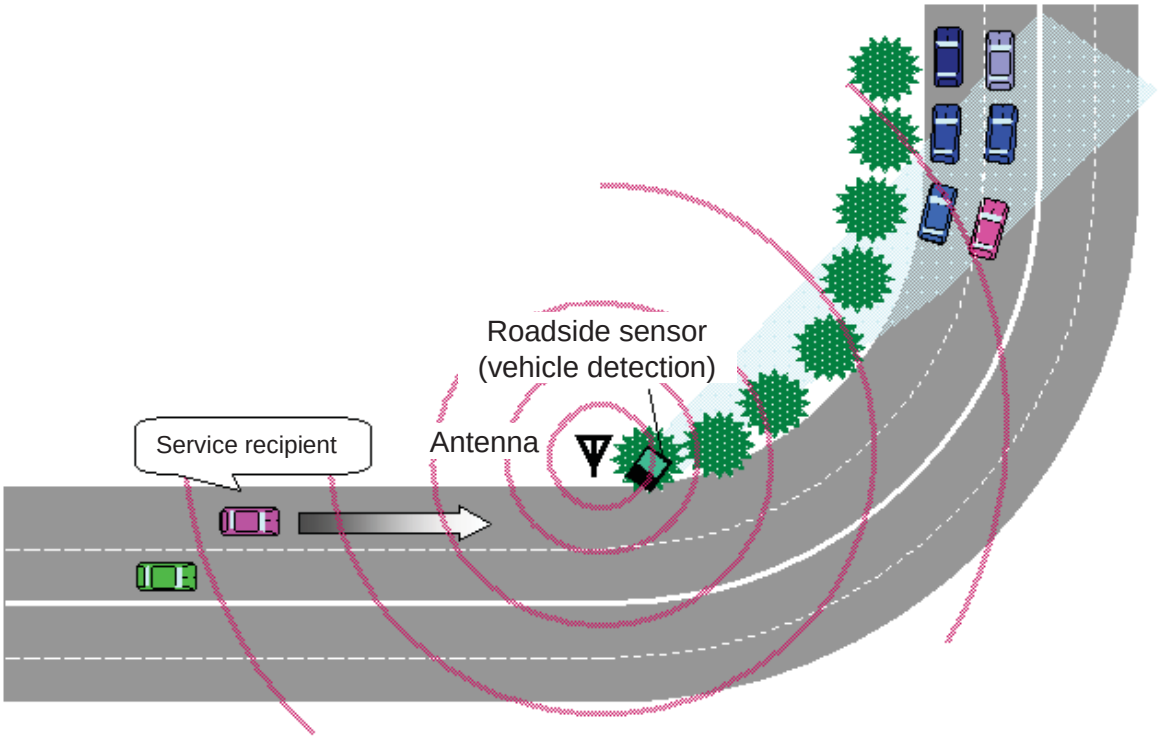


Figure 2-10: Service scenario for prevention of rear end collision

2.2.5 Prevention of failure to notice pedestrians at a crossing

・Service outline

A roadside sensor or similar detects the presence of pedestrians at a crossing, and the information is provided to the drivers of vehicles attempting to make a right or left turn.

・Service scenario

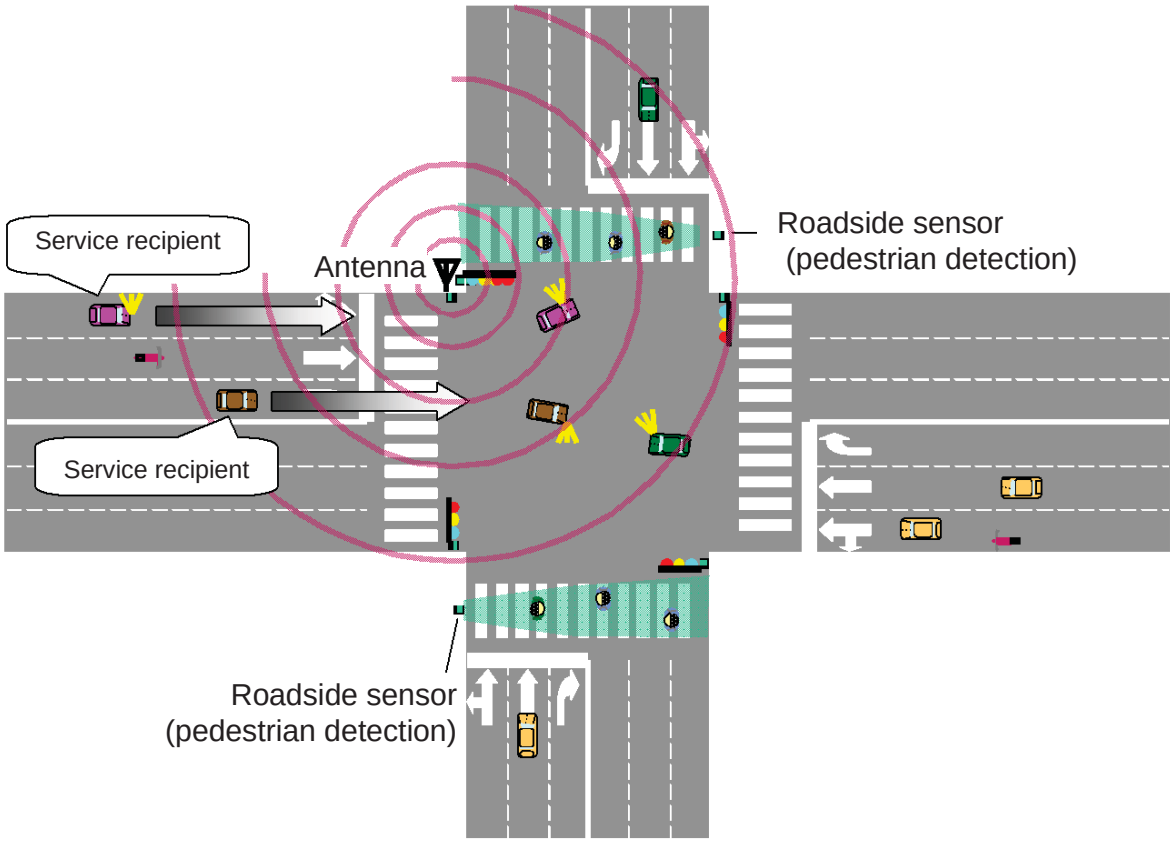


Figure 2-1: Service scenario for prevention of failure to notice pedestrians at a crossing

2.2.6 Prevention of failure to notice traffic signals

・Service outline

At an intersection with traffic signals, information about the signal light state is provided to vehicle drivers, to prevent accidents due to failing to notice a red light.

・Service scenario

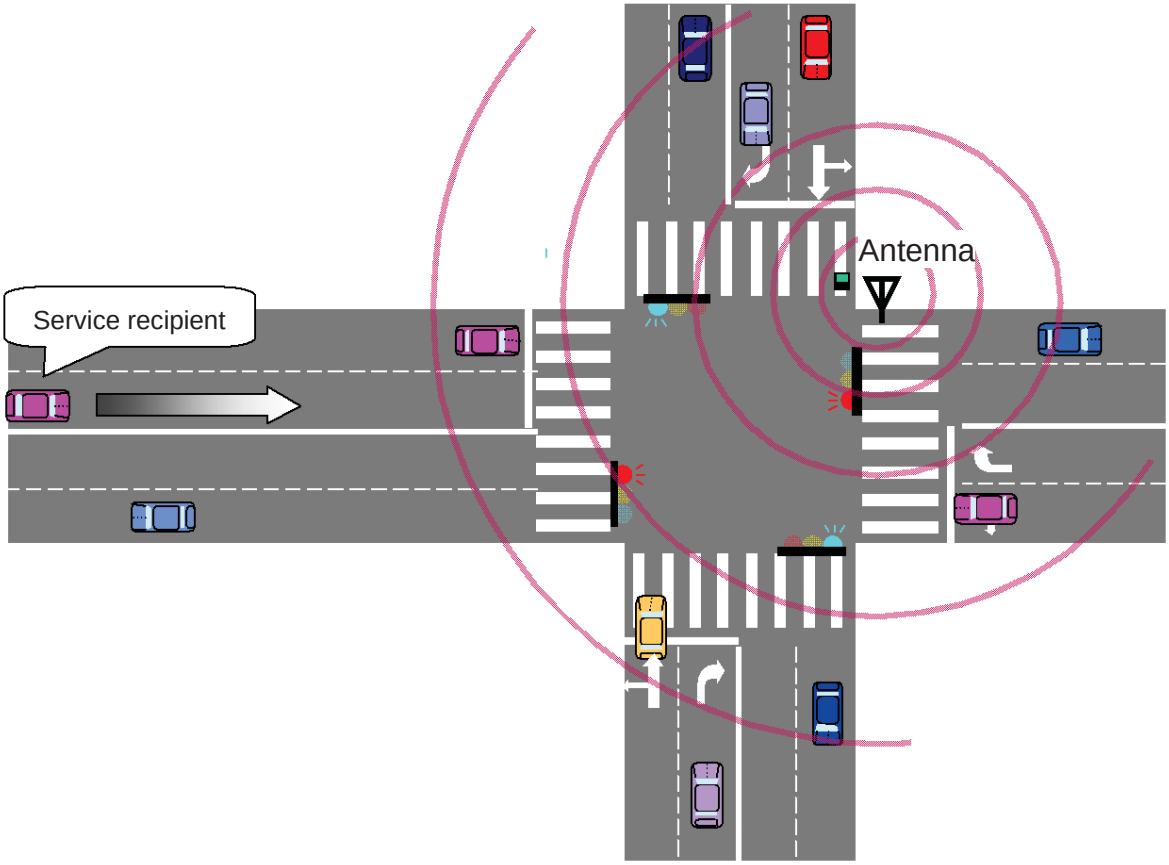


Figure 2-2: Service scenario for prevention of failure to notice traffic signals

2.2.7 Prevention of failure to notice a stop sign

・Service outline

At an intersection without traffic signals, information about the stopping requirement or other rule is provided to vehicle drivers, to prevent accidents due to failing to notice the stop sign.

・Service scenario

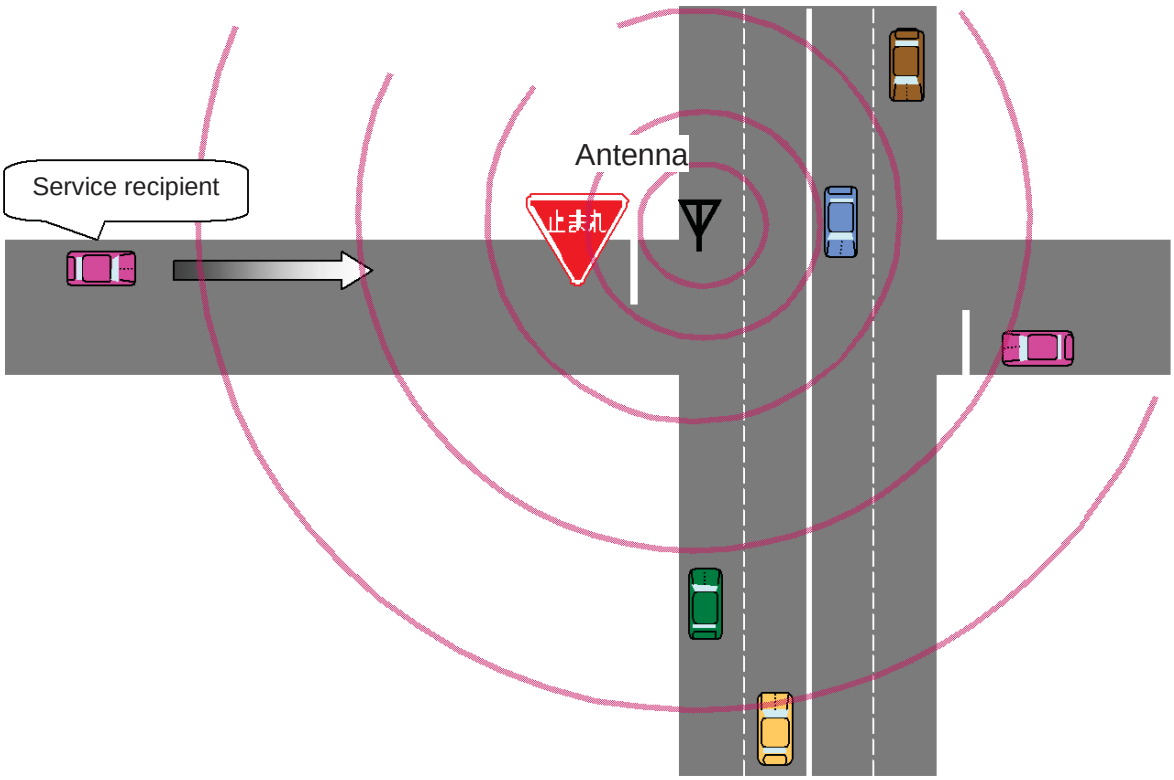


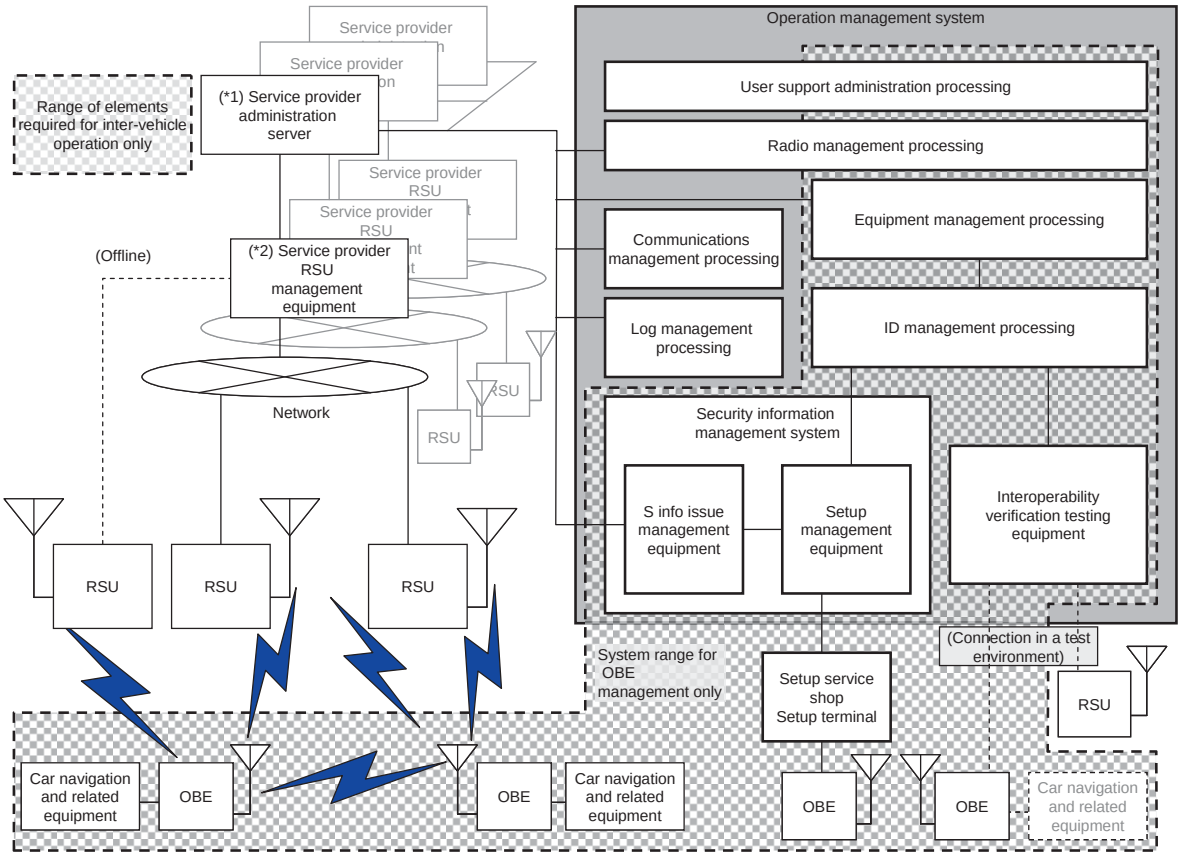
Figure 2-3: Service scenario for prevention of failure to notice stop sign

[Blank]

Chapter 3: Driver Assistance Communications System Configuration

The diagram below shows the configuration of a system comprising the elements required to realize the practical services listed in the preceding chapter.

The general concept of the system envisioned by this guideline is also represented in Figure 3-1, with multiple service providers owning different RSUs, and the equipment and servers used to manage these being linked to the respective equipment of the operation management organization. Also belonging to the configuration is OBE owned by users and connected to the infrastructure equipment. The elements required by service providers not using RSUs and operating solely through OBE are grouped in the section of the configuration diagram enclosed by a broken line.



(*1) Service provider administration server: dedicated equipment for each service provider, implementing security and providing control, radio and communications management. Directly managed by the service provider. correct operation
(*2) Service provider RSU management equipment: Equipment owned by service provider and used for control of RSUs.

Figure 3-1: System Configuration Diagram

[Blank]

Chapter 4: System Threat and Risk Analysis

Possible threats to the system described in the preceding chapter need to be identified, and risk analysis must be performed. The procedures for these tasks are described below.

For this analysis, in order to look into security methods for roadside-to-vehicle and inter-vehicle communication, the communication paths between RSU and OBE, and between multiple OBEs, including the equipment used for communication, need to be considered.

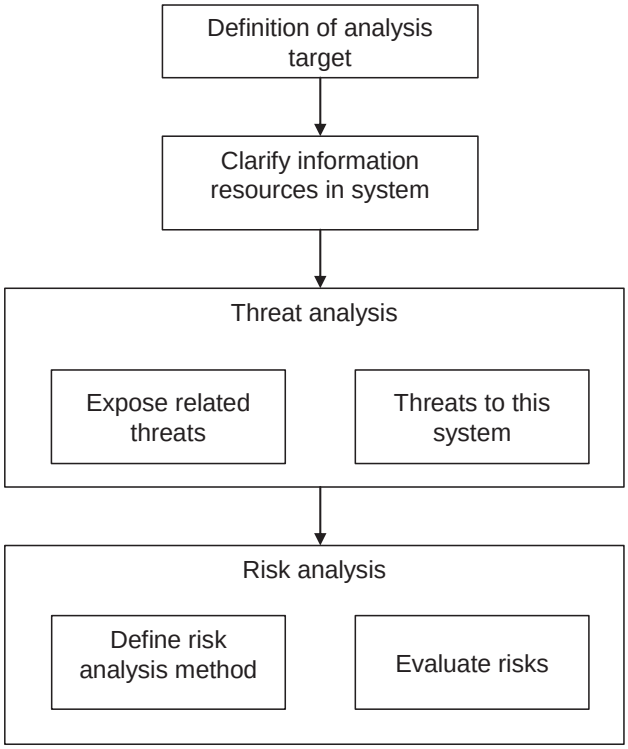


Figure 4-1: Threat and risk analysis procedure

The results of analysis performed according to the above procedure are described in this chapter.

4.1 Definition of analysis target

As shown in Figure 4-2, the targets for analysis are the communication paths between RSU and OBE, and between multiple OBEs. The type of communication is broadcast communication. With regard to RSUs, roadside sensors for detection of pedestrians or two-wheeled vehicles, as well as traffic signals and similar are not included in the analysis. Because the system is aimed at providing driving safety assistance, roadside-to-vehicle communication for billing purposes is also excluded.

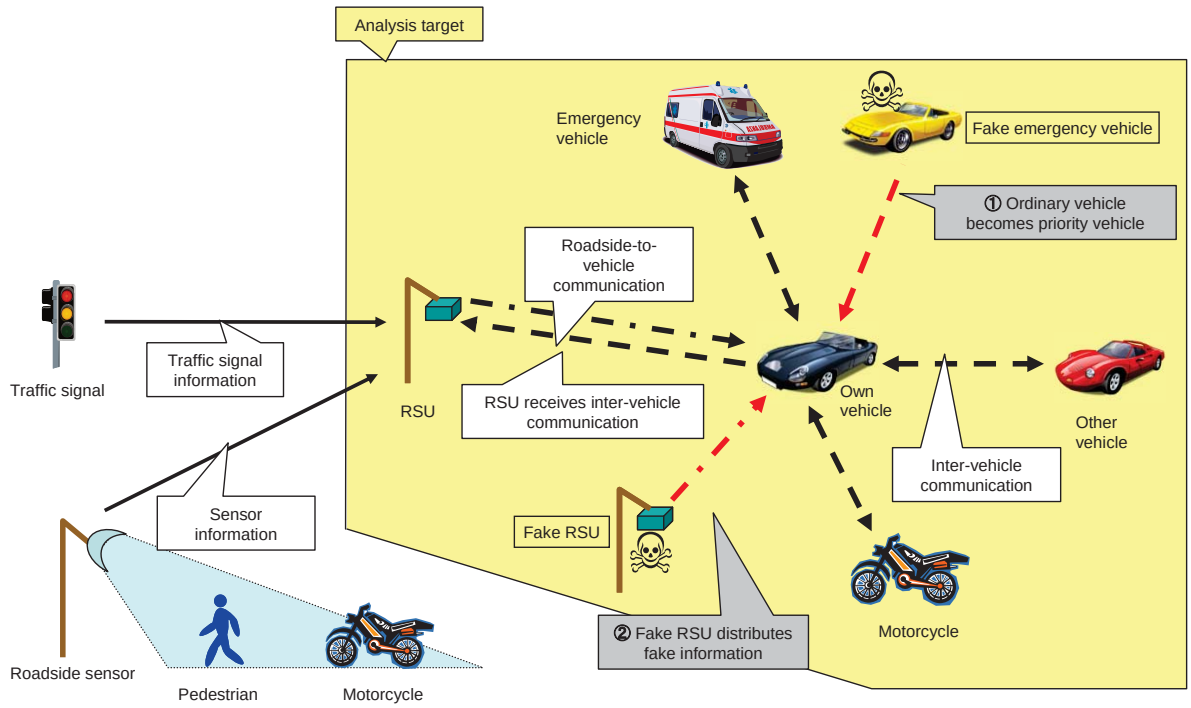


Figure 4-2: Analysis targets

As can be seen from the illustration, the following types of threats exist in the above system:

1. An ordinary vehicle emits fake priority information and makes itself appear to be a priority vehicle (e.g. energency vehicle)

2. A fake RSU distributes fake information (e.g. contradictory information to preceding and following vehicles)

These and similar threats may cause confusion, for example regarding the presence of priority vehicles outside of one's field of vision, or through the reception of fake messages, possibly resulting in accidents. Consequently, roadside-to-vehicle communication and inter-vehicle communication within the driver assistance communications system needs to be secured.

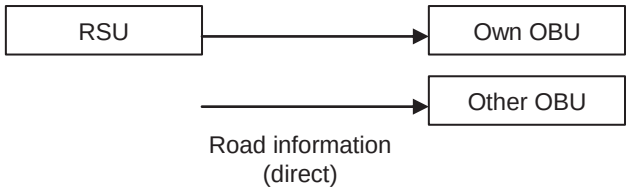
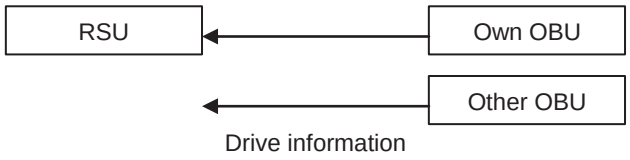
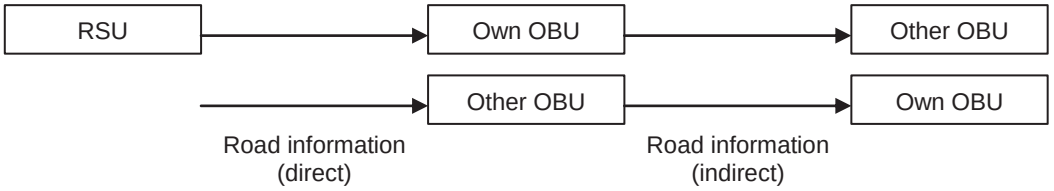
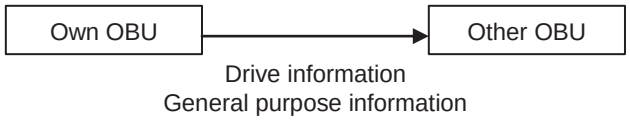
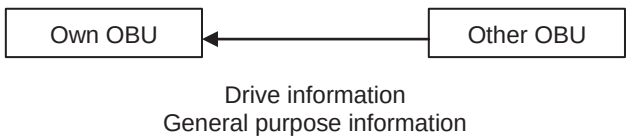
4.2 Information resources in system

Table 4-1 shows information resources and communication patterns for inter-vehicle and roadside-to-vehicle communication.

Information distributed directly from a RSU to OBE is called "road information (direct)," consisting of management information such as RSU transmission time allotment, etc. and RSU information such as traffic signal information, traffic condition information, etc.

Information distributed by OBE to RSUs and other OBE comprises drive information, general information, and relayed information from other RSUs, is summarily called “road information (indirect).” Drive information includes data about vehicle position and speed, vehicle type, current operation status in case of emergency vehicles, and other driving related information. General information is information that can be accessed freely by other vehicles. Road information (indirect) is communication management information that is part of road information (direct), received by OBE from a RSU and altered for relaying to other OBE.

Table 4-1: Communication cases and communication information

Case	Communication case and communication information	Remarks
①		—
②		Information from inter-vehicle communication received by RSU
③		Relaying of information sent by RSU
④		—
⑤		—

4.3 Threat analysis

In order to compile a list of possible threats to the system of roadside-to-vehicle communication and inter-vehicle communication, published papers (reference material [2] – [6]) were examined. The results are shown in Table 4-2.

Table 4-2: List of possible threats

ID	Threat	Description
1	DoS	Denial of Service attack by sending a large number of messages to RSUs and/or OBE
2	Jamming	Impeding radio communication by using equipment broadcasting on the same frequency
3	Malware	Infecting OBE and/or RSUs with a virus (including during update)
4	Replay attack	Re-using previously used messages
5	Spam	Sending spam messages
6	Falsification of external information	Falsification of information from external sources (speed and position, time, pedestrian detection, etc.) used by OBE and/or RSUs
7	False GPS signal	Misuse of GPS signal emitter to send a false GPS signal
8	Spoofing (1)	Spoofing a RSU
9	Spoofing (2)	Spoofing other OBE or priority vehicle
10	False message transmission	Sending faked messages
11	Message falsification	Modifying messages
12	Eavesdropping	Interception of communication data by persons inside or outside the network
13	Location tracking	Obtaining individual position information from reception data by persons inside or outside the network
14	Black hole	Purposely not forwarding (or delaying) information to be forwarded
15	Equipment falsification	Falsification of software, internal data, or send messages of OBE and/or RSUs

Within the context of the system described in the preceding chapter, the above threats were analyzed with regard to the information resources described in section 4.2. The results are shown in Table 4-3. Some of the threats in Table 4-2 are related to other threats (e.g. spoofing by replay attack). These are treated together in Table 4-3.

The numbers in brackets in the table appended to the threat name refer to the IDs in Table 4-2.

Table 4-3: Threat analysis

Information resource	Threat		Description
Road information Drive information General purpose information	Dos (1)		Disabling the system by sending a large number of messages, either by a third party using communication equipment or by a user misusing OBE
	Jamming (2)		A third party disabling the system by emitting radio signals designed to create interference
	False GPS signal (7)		A third party misusing a GPS signal generator to distribute messages containing false position information, with the aim of creating confusion
	Malware (3)		A third party or a user misusing communication messages, or service personnel (regardless of presence or absence of malicious intent) or third parties physically accessing RSUs or OBE to infect the equipment and send false messages with the aim of creating confusion or disabling the system
	Falsification of external information (6)		Falsification of input information for OBE by a user or service personnel (regardless of presence or absence of malicious intent), or falsification of input information for RSU by service personnel (regardless of presence or absence of malicious intent) or a third party, to distribute messages containing wrong information with the aim of creating confusion
	Eavesdropping (12)		Misuse of OBE by user or use of communication equipment by a third party to obtain confidential information comprised in general purpose information (drive information and road information is broadcast to all OBE and contains no confidential information)
			Use of communication equipment by a third party to receive communication messages and use them for services not intended by operation management organization (depends on policy of operation management organization)
	Equipment falsification (15)		A third party, a user, or service personnel (regardless of presence or absence of malicious intent) disassembling or modifying OBE or a RSU to modify the software or data of the OBE or RSU. This may involve the distribution of false messages to cause confusion or disable the system.
Road information (direct)	RSU spoofing (8)	Sending false road information (10)	Misuse of OBE by user or use of communication equipment by a third party to appear as a RSU and distribute road information containing wrong information, with the aim of creating confusion
		Replay attack (4)	Re-using of information distributed by a RSU to appear as a RSU and create confusion through re-used messages
Drive information General purpose information	Vehicle spoofing (8, 9)	Sending false drive information (10)	Misuse of OBE by user or use of communication equipment by a third party to appear as another vehicle (including emergency vehicle) and distribute drive information containing wrong information, with the aim of creating confusion
		Sending false general purpose information (10)	Misuse of OBE by user or use of communication equipment by a third party to appear as another vehicle and distribute general purpose information containing wrong information, with the aim of creating confusion

Information resource	Threat		Description
		Replay attack (4)	Re-using of correct information distributed by another vehicle to appear as another vehicle and create confusion through re-used messages
	Location tracking (13)		Use of communication equipment by a third party, misuse of OBE by a user, or misuse of a RSU by service personnel to trace the location of an individual through received messages, with the aim of individual profiling (privacy invasion)
Road information (indirect)	Falsification by relay vehicle (11)		Modification of information distributed by a RSU and transmitting the result with the aim of obstructing inter-vehicle communication and/or roadside-to-vehicle communication
	Sending false road information (indirect) (10)		Misuse of OBE by a user, or use of communication equipment by a third party to transmit road information (indirect) in a location where no RSU is installed, to spoof the presence of a RSU to OBE and obstruct inter-vehicle communication

Threats listed in Table 4-2 but not included in Table 4-3 and therefore not considered here are as follows:

- Spam (5): This threat involves the possible distribution of unauthorized advertising or other messages in inter-vehicle and/or roadside-to-vehicle communication. It is excluded because advertising services are not covered here.

- Spam (5): This threat involves the possible distribution of unauthorized advertising or other messages in inter-vehicle and/or roadside-to-vehicle communication. It is excluded because advertising services are not covered here.

4.4 Risk analysis

The threats analyzed in Table 4-3 were subject to risk analysis.

4.4.1 Risk analysis method

The method described in reference [2] was used for risk analysis.

This method is an improved version of the ETSI (European Telecommunications Standard Institute) method. It is described below.

The risk value is the product of the occurrence likelihood value and the impact value. The definitions of occurrence likelihood and impact are given in Table 4-4. The method is the ETSI method.

Table 4-4: Definition of occurrence likelihood and impact

Item	Rating	Value	Definition
Occurrence likelihood	Likely	3	All elements are present
	Possible	2	Some elements are present
	Unlikely	1	Important elements are missing
Impact	High	3	Serious consequences for users and service
	Medium	2	Short-term service stoppage occurs
	Low	1	Some consequences for users and service

The method used in reference [2] further divides the occurrence likelihood defined in reference [7] into motive and technical difficulty. The definitions of motive and technical difficulty are as follows:

Table 4-5: Definition of motive and technical difficulty

Item	Rating	Value
Motive	High	Potential for large gain (financial or otherwise) by attacking person or organization
	Moderate	Creating confusion in the service (crime committed for fun, etc.)
	Low	Potential for gain is low
Technical difficulty	None	Attack can easily be performed, on technical and economical level (precedents exist)
	Solvable	Attack is possible in theory
	Strong	Attack is very difficult, on theoretical, technical, and economical level

Taking the above two factors into account, the relationship to the risk value is as shown below. The risk value is defined as follows:

Risk value (9,6) → Critical: Countermeasure is mandatory

(4) → Major: Requires attention

(3,2,1) → Minor: Immediate countermeasure is not necessary

Table 4-6: Definition of risk value

<table>
<tr><th rowspan="2">Motive</th><th rowspan="2">Technical difficulty</th><th rowspan="2">Occurrence likelihood</th><th colspan="3">Impact</th></tr>
<tr><th>High(3)</th><th>Medium(2)</th><th>Low(1)</th></tr>
<tr><td rowspan="2">High</td><td>None</td><td rowspan="3">Likely(3)</td><td rowspan="3">Critical(9,6)</td><td rowspan="2"></td><td rowspan="3"></td></tr>
<tr><td>Solvable</td></tr>
<tr><td rowspan="2">Moderate</td><td>None</td></tr>
<tr><td>Solvable</td><td>Possible(2)</td><td>Major(4)</td></tr>
<tr><td>Low</td><td>Any</td><td rowspan="2">Unlikely(1)</td><td colspan="3" rowspan="2"></td></tr>
<tr><td>Any</td><td>Strong</td><td>Minor(3,2,1)</td></tr>
</table>

4.4.2 Risk analysis results

Using the above method, risk analysis was performed for the threats listed in section 4.3, in order to determine the risk value. The results are shown in Table 4-8.

The IDs used in this table are newly assigned identifiers which correspond to the reasons indicated further below. The abbreviations shown in Table 4-7 were used.

Table 4-7: Abbreviations used in subsequent tables

Item	Term	Abbreviation
Motive	High	High
	Moderate	Mod.
	Low	Low
Technical difficulty	None	None
	Solvable	Sol.
	Strong	Str.
Occurrence likelihood	Likely	Like.
	Possible	Poss.
	Unlikely	Unl.
Impact	High	High
	Medium	Med.
	Low	Low

Item	Term	Abbreviation
Risk value	Critical	Crt.
	Major	Maj.
	Minor	Min.

The current analysis treats attacks where the attack method or main attacker differs separately, and it was assumed that service personnel would not commit an illegal act (motive was set to “Low”).

In the process of realizing the service, the results of this risk analysis will have to be reviewed by the operation management organization and the service providers.

Table 4-8: Risk analysis results

ID	Threat	Description	Motive	Technical difficulty	Occurrence likelihood	Impact	Risk value
A	DoS	Disabling the system by sending a large number of messages, either by a third party using communication equipment or by a user misusing OBE	Mod.	Sol.	Poss. (2)	Med. (2)	Maj. (4)
B	Jamming	A third party disabling the system by emitting radio signals designed to create interference	Mod.	None	Like. (3)	Med. (2)	Crt. (6)
C	False GPS signal	A third party misusing a GPS signal generator to distribute messages containing false position information, with the aim of creating confusion	Mod.	Sol.	Poss. (2)	Med. (2)	Maj. (4)
D	Malware (1)	A third party or a user misusing communication messages or using physical access to infect RSUs or OBE and send false messages with the aim of creating confusion or disabling the system	Mod.	Sol.	Poss. (2)	High (3)	Crt. (6)

ID	Threat	Description	Motive	Technical difficulty	Occurrence likelihood	Impact	Risk value
E	Malware (2)	Service personnel using physical access to infect RSUs or OBE and send false messages with the aim of creating confusion or disabling the system	Low	Sol.	Unl. (1)	High (3)	Min. (3)
F	Falsification of external information (1)	Falsification of input information for OBE by a user, or falsification of input information for a RSU by a third party, to distribute messages containing wrong information, with the aim of creating confusion	Mod.	Sol.	Poss. (2)	High (3)	Crt. (6)
G	Falsification of external information (2)	Falsification of input information for OBE or a RSU by service personnel, to distribute messages containing wrong information, with the aim of creating confusion	Low	Sol.	Unl. (1)	High (3)	Min. (3)
H	Eavesdropping (1)	Misuse of OBE by user or use of communication equipment by a third party to obtain confidential information comprised in general purpose information (drive information and road information is broadcast to all OBE and contains no confidential information)	—	Sol.	—	—	— (See below)

ID	Threat	Description	Motive	Technical difficulty	Occurrence likelihood	Impact	Risk value
I	Eavesdropping (2)	Use of communication equipment by a third party to receive communication messages and use them for services not intended by operation management organization (depends on policy of operation management organization)	High	Sol.	Like. (3)	Low (1)	Min. (3)
J	Equipment falsification (1)	Third party or user disassembling or modifying OBE or a RSU to modify the software or data of the OBE or RSU. This may involve the distribution of false messages to cause confusion or disable the system.	Mod.	Sol.	Poss. (2)	High (3)	Crt. (6)
K	Equipment falsification (2)	Service personnel disassembling or modifying OBE or a RSU to modify the software or data of the OBE or RSU. This may involve the distribution of false messages to cause confusion or disable the system.	Low	Sol.	Unl. (1)	High (3)	Min. (3)
L	RSU spoofing Sending false road information	Misuse of OBE by user or use of communication equipment by third party to appear as a RSU and distribute road information containing wrong information, with the aim of creating confusion	Mod.	Sol.	Poss. (2)	Med. (2)	Maj. (4)
M	RSU spoofing Replay attack	Re-using of information distributed by a RSU to appear as a RSU and create confusion through re-used messages	Mod.	None	Like. (3)	Med. (2)	Crt. (6)

ID	Threat	Description	Motive	Technical difficulty	Occurrence likelihood	Impact	Risk value
N	Vehicle spoofing Sending false drive information	Misuse of OBE by user or use of communication equipment by third party to appear as another vehicle (including emergency vehicle) and distribute drive information containing wrong information, with the aim of creating confusion	Mod.	Sol.	Poss. (2)	Med. (2)	Maj. (4)
O	Vehicle spoofing Sending false general purpose information	Misuse of OBE by user or use of communication equipment by third party to appear as another vehicle and distribute general purpose information containing wrong information, with the aim of creating confusion	Mod.	Sol.	Poss. (2)	Med. (2)	Maj. (4)
P	Vehicle spoofing Replay attack	Re-using of correct information distributed by another vehicle to appear as another vehicle and create confusion through re-used messages	Mod.	None	Like. (3)	Med. (2)	Crt. (6)
Q	Location tracking (1)	Use of communication equipment by a third party, or misuse of OBE by a user to trace the location of an individual through received messages, with the aim of individual profiling (privacy invasion)	High	Sol.	Like. (3)	Low (1)	Min. (3)
R	Location tracking (2)	Misuse of RSU by a third party to trace the location of an individual through received messages, with the aim of individual profiling (privacy invasion)	High	Str.	Unl. (1)	Low (1)	Min. (1)

ID	Threat	Description	Motive	Technical difficulty	Occurrence likelihood	Impact	Risk value
S	Location tracking (3)	Misuse of a RSU by service personnel to trace the location of an individual through received messages, with the aim of individual profiling (privacy invasion)	Low	Str.	Unl. (1)	Low (1)	Min. (1)
T	Modification by relay vehicle	Modification of information distributed by a RSU and transmitting the result with the aim of obstructing inter-vehicle communication and/or roadside-to-vehicle communication	Mod.	Sol.	Poss. (2)	Med. (2)	Maj. (4)
U	Sending false road information (indirect)	Misuse of OBE by a user, or use of communication equipment by a third party to transmit road information (indirect) in a location where no RSU is installed, to spoof the presence of a RSU to OBE and obstruct inter-vehicle communication	Mod.	Sol.	Poss. (2)	Med. (2)	Maj. (4)

The reasons for the risk analysis results shown in Table 4-8 are given in Table 4-9.

Table 4-9: Risk analysis reasons

ID	Threat	Item	Rating	Reason
A	DoS	Motive	Moderate	Aiming for confusion
		Difficulty	Solvable	Precedents for attack exist in wired systems. In wireless systems, the possibility for attack is present in theory.
		Impact	Medium	Impact is limited to location of attack.
B	Jamming	Motive	Moderate	Aiming for confusion
		Difficulty	None	Precedents for attack exist.
		Impact	Medium	Impact is limited to location of attack.
C	False GPS signal	Motive	Moderate	Aiming for confusion
		Difficulty	Solvable	Attack is possible in theory.
		Impact	Medium	Impact is limited to location of attack.
D	Malware (1)	Motive	Moderate	Aiming for confusion
		Difficulty	Solvable	Attack is possible in theory.
		Impact	High	Impact may spread to entire system. Removal is mandatory.
E	Malware (2)	Motive	Low	Service personnel do not have a motive.
		Difficulty	Solvable	Attack is possible in theory.
		Impact	High	Impact may spread to entire system. Removal is mandatory.
F	Falsification of external information (1)	Motive	Moderate	Aiming for confusion
		Difficulty	Solvable	Attack is possible in theory.
		Impact	High	Modification after falsification is necessary.
G	Falsification of external information (2)	Motive	Low	Service personnel do not have a motive.
		Difficulty	Solvable	Attack is possible in theory.
		Impact	High	Modification after falsification is necessary
H	Eavesdropping (1)	Motive	—	As general purpose information is not known, evaluation is not possible (see below).
		Difficulty	Solvable	Attack is possible in theory.

ID	Threat	Item	Rating	Reason
		Impact	—	As general purpose information is not known, evaluation is not possible (see below).
I	Eavesdropping (2)	Motive	High	Aiming for profit from selling unauthorized OBE
		Difficulty	Solvable	Attack is possible in theory.
		Impact	Low	No impact on regular users and services. May become a threat depending on policy of operation management organization.
J	Equipment falsification (1)	Motive	Moderate	Aiming for confusion
		Difficulty	Solvable	Attack is possible in theory.
		Impact	High	Modification after falsification is mandatory.
K	Equipment falsification (2)	Motive	Low	Service personnel do not have a motive.
		Difficulty	Solvable	Attack is possible in theory.
		Impact	High	Modification after falsification is mandatory.
L	RSU spoofing, sending false road information	Motive	Moderate	Aiming for confusion
		Difficulty	Solvable	Attack is possible in theory.
		Impact	Medium	Impact is limited to location where sending takes place.
M	RSU spoofing, replay attack	Motive	Moderate	Aiming for confusion
		Difficulty	None	Precedents for attack exist.
		Impact	Medium	Impact is limited to location of attack.
N	Vehicle spoofing, sending false drive information	Motive	Moderate	Aiming for confusion
		Difficulty	Solvable	Attack is possible in theory.
		Impact	Medium	Impact is limited to location where sending takes place.
O	Vehicle spoofing, sending false general purpose information	Motive	Moderate	Aiming for confusion
		Difficulty	Solvable	Attack is possible in theory.
		Impact	Medium	Impact is limited to location where sending takes place.
P	Vehicle spoofing, replay attack	Motive	Moderate	Aiming for confusion
		Difficulty	None	Precedents for attack exist.
		Impact	Medium	Impact is limited to location of attack.

ID	Threat	Item	Rating	Reason
Q	Location tracking (1)	Motive	High	Clear aim (profiling of specific individual) with potential for large gain.
		Difficulty	Solvable	Attack is possible in theory.
		Impact	Low	Impact on specific individual, tracing within communication range is required, similar to stalking (see below).
R	Location tracking (2)	Motive	High	Clear aim (profiling of specific individual) with potential for large gain.
		Difficulty	Strong	Necessity for misuse of multiple RSUs makes attack difficult (see below).
		Impact	Low	Impact on specific individual
S	Location tracking (3)	Motive	Low	Service personnel do not have a motive.
		Difficulty	Strong	Necessity for misuse of multiple RSUs makes attack difficult (see below).
		Impact	Low	Impact on specific individual
T	Modification by relay vehicle	Motive	Moderate	Aiming for confusion
		Difficulty	Solvable	Attack is possible in theory.
		Impact	Medium	Impact is limited to location of attack (see below).
U	Sending false road information (indirect)	Motive	Moderate	Aiming for confusion
		Difficulty	Solvable	Attack is possible in theory.
		Impact	Medium	Impact is limited to location of attack (see below).

In the following, additional reasons to those shown in Table 4-9 are given for eavesdropping of general purpose information broadcast by OBE (H), location tracking of drive information and general purpose information (Q and R), relay vehicle modification for relay of road information (indirect) from OBE or RSUs to other OBE (T), and sending of false road information (indirect) (U).

- Eavesdropping of general purpose information

Because the content and intent of general purpose information at this point is undecided, the motive of possible attackers and the impact of possible attacks cannot be evaluated properly. Consequently, security countermeasures must be considered once these aspects have been

decided, according to the characteristics of the services to be provided.

- Location tracking

As illustrated in Figure 4-3, location tracking can consist in disclosing the fact that vehicle A has visited the locations X→Y→Z, and using this information to perform profiling of an individual. Vehicle A is taken to carry OBE for this system, and therefore broadcasting unique identification information (e.g. OBE ID, MAC address, etc.) as well as position information, etc. In this condition, the possible impact of location tracking has been defined as “Low” for the following reasons.

A. Misuse of OBE and communication equipment

A vehicle which does location trackking ("location tracker") can track (1) the identity of vehicle A and (2) its position from A's broadcast messages. However, for continuous tracking, the location tracker needs to remain within the communication range of the vehicle A , which is the same as stalking.

B. Misuse of RSU

The RSU D can identify the vehicle. However, because this applies only to vehicles within the communication range of the RSU, location tracking is not possible. Location tracking through misuse of multiple RSUs is in theory possible, but since the destination of the vehicle is unknown, this would require control over all RSUs, which is highly unlikely. (Breaking into the RSU server to obtain the information would be more efficient.)

C. Misuse of RSU server

This is outside the scope of the current analysis, but tracking of (1) the identity of vehicle A and (2) its position would be possible if there is a centralized server that collects all messages obtained by RSUs, and if this server is either hacked or under the control of a malicious operator. Consequently, measures against intrusion must be implemented, such as a management method that obscures the correlation of vehicle⇔OBE ID⇔position, or separate operation assigning of vehicle⇔ID and ID⇔position.

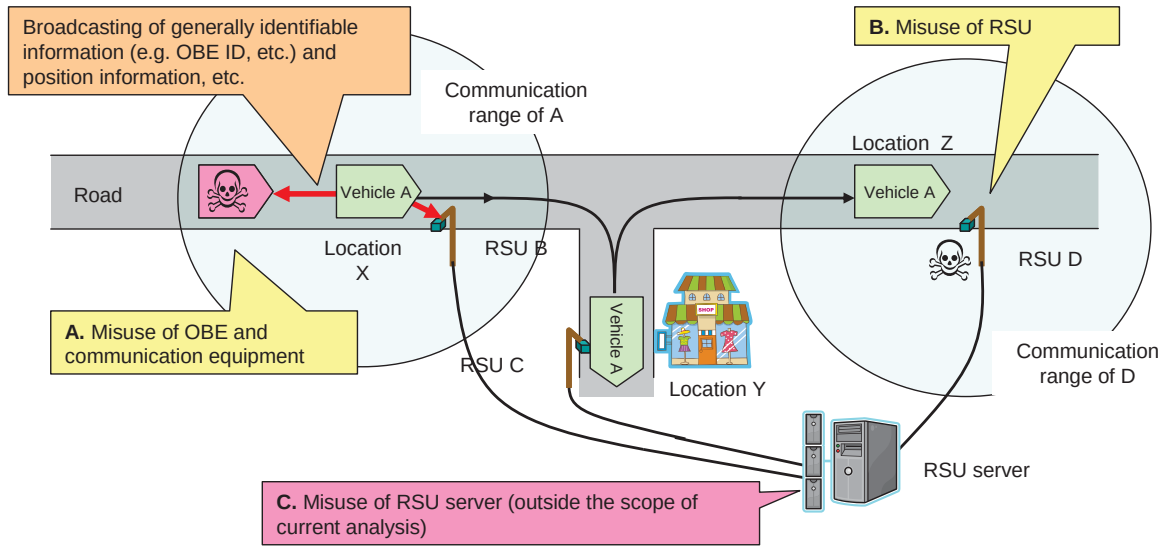


Figure 4-3: Location tracking

- Modification by relay vehicle and sending of false road information (indirect)

This is a threat whereby a vehicle having received road information (direct) from a RSU relays this to another vehicle as road information (indirect) in modified form, or relays road information (indirect) although no road information (direct) was received (i.e. corresponding RSU does not exist). Road information (indirect) is used for communication management to allocate sending time to RSUs and other tasks. By receiving this information indirectly from other vehicles, a vehicle not directly in the range of a RSU can know the existence of a RSU in the vicinity. If this road information (indirect) has been modified by the relaying vehicle, the possible impact has been ranked as "Medium", due to the following limiting factors:

1) If the sending time of the RSU is long but has been falsified as short, the vehicle receiving the falsified information will carry out inter-vehicle communication during the differential interval, so that vehicles that are both within the communication range of the RSU and within the communication range of the vehicle that has received falsified information will be unable to communicate correctly.

2) If the sending time of the RSU is short or zero, but has been falsified as long, the vehicle receiving the falsified information may not distribute road information or general purpose information during the differential interval, and may not carry out inter-vehicle communication.

4.5 Conclusion

Possible countermeasure policies for the threats shown in Table 4-8 under the aspects of

communication, equipment, and operation are listed in Table 4-10. This table only covers threats ranked “Critical” or “Major.” Threats ranked “Minor” have been excluded. Threats related to eavesdropping of general purpose information have also been excluded for the reason explained above. Countermeasures for eavesdropping (2) have been included, for the reason stated later in this section.

Table 4-10: Threats requiring countermeasures and security measures

ID	Threat	Risk value	Countermeasure policy			Remarks
			Communications	Equipment	Operation	
A	DoS	Major(4)	—	Making OBE tamper-proof	Legal measures or other regulations	—
B	Jamming	Critical(6)	—	—	Legal measures or other regulations	—
C	False GPS signal	Major(4)	—	—	Legal measures or other regulations	—
D	Malware (1)	Critical(6)	—	Blocking reception of irregular data (implementation level) Making RSUs and OBE tamper-proof	—	—
E	Malware (2)	Minor(3)	—	—	—	—
F	Falsification of external information (1)	Critical(6)	—	Making RSUs tamper-proof	Vehicle inspection	See below
G	Falsification of external information (2)	Minor(3)	—	—	—	—
H	Eavesdropping (1)	—	—	—	—	—
I	Eavesdropping (2)	Minor(3)	Maintaining message confidentiality	—	Certification framework	See below

ID	Threat	Risk value	Countermeasure policy			Remarks
			Communications	Equipment	Operation	
J	Equipment falsification (1)	Critical(6)	—	Making OBE and RSUs tamper-proof	—	—
K	Equipment falsification (2)	Minor(3)	—	—	—	—
L	RSU spoofing Sending false road information	Major(4)	Verification of sender authenticity Verification of message integrity	Making OBE tamper-proof	—	—
M	RSU spoofing Replay attack	Critical(6)	Verification of sender authenticity	—	—	See below
N	Vehicle spoofing Sending false drive information	Major(4)	Verification of sender authenticity Verification of message integrity	Making OBE tamper-proof	—	—
O	Vehicle spoofing Sending false general purpose information	Major(4)	Verification of sender authenticity Verification of message integrity	Making OBE tamper-proof	—	—
P	Vehicle spoofing Replay attack	Critical(6)	Verification of sender authenticity	—	—	See below
Q	Location tracking (1)	Minor(3)	—	—	—	—
R	Location tracking (2)	Minor(1)	—	—	—	—
S	Location tracking (3)	Minor(1)	—	—	—	—
T	Modification by relay vehicle	Major(4)	Verification of received data integrity	—	Regulating roadside-to-vehicle communication time	See below
U	Sending false road information (indirect)	Major(4)	Verification of received data integrity	—	Regulating roadside-to-vehicle communication time	See below

Additional explanations for the threats marked “See below” in Table 4-10 are given in the

following section:

- Falsification of external information (1)

If information such as speed data input to the OBE has been modified, security measures of the communication system and equipment will not be able to contain the resulting threat. Consequently, a framework that allows unique identification of the OBE that is distributing messages comprising falsified information by authenticity checking is required.

- Eavesdropping (2)

Because this is dependent on applicability to other services and the policy of the operation management organization, maintaining confidentiality as a system must be possible.

- Replay attacks

In concrete terms, countermeasures will involve checking the message sending time or similar measures. These are included in the category of sender authenticity checking.

- Modification by relay vehicle and sending of false road information (indirect)

Countermeasures in the communications category involve verification that received data match the communication standard and rejection of data that fail the verification. In order to prevent interference with inter-vehicle communication, the time ratio (maximum value) of roadside-to-vehicle communication should be defined in the operation category (see Annex C). Because the above communications related countermeasure is linked to communication specifications, the topic is not further dealt with in this document.

Based on the above threats and risk analysis results, threats that require communications related countermeasures are spoofing and sending of false information as well as replay attacks. These countermeasures involve maintaining message confidentiality, verifying the authenticity of the sender, and checking for message integrity.

[Blank]

Chapter 5: Security Related Countermeasure Policy

The policies for countermeasures against the threats listed in the preceding chapter are as follows:

1. Use encryption technology for inter-vehicle and roadside-to-vehicle communication, in order to verify the authenticity of the sender and the integrity of messages. Also enable the capability to maintain confidentiality of information being carried in the communication link. The encryption algorithm is to be chosen from the CRYPTREC list of recommended cryptographic techniques for government and industrial use.
2. If keys used for the above purposes of authenticity checking, integrity checking, and confidentiality maintenance have been leaked, countermeasures for minimizing the impact and preventing further spread must be available.
3. Information other than that exchanged during inter-vehicle and roadside-to-vehicle communication, as well as information stored in equipment must be properly protected by the entity managing communication lines and equipment in the respective link.

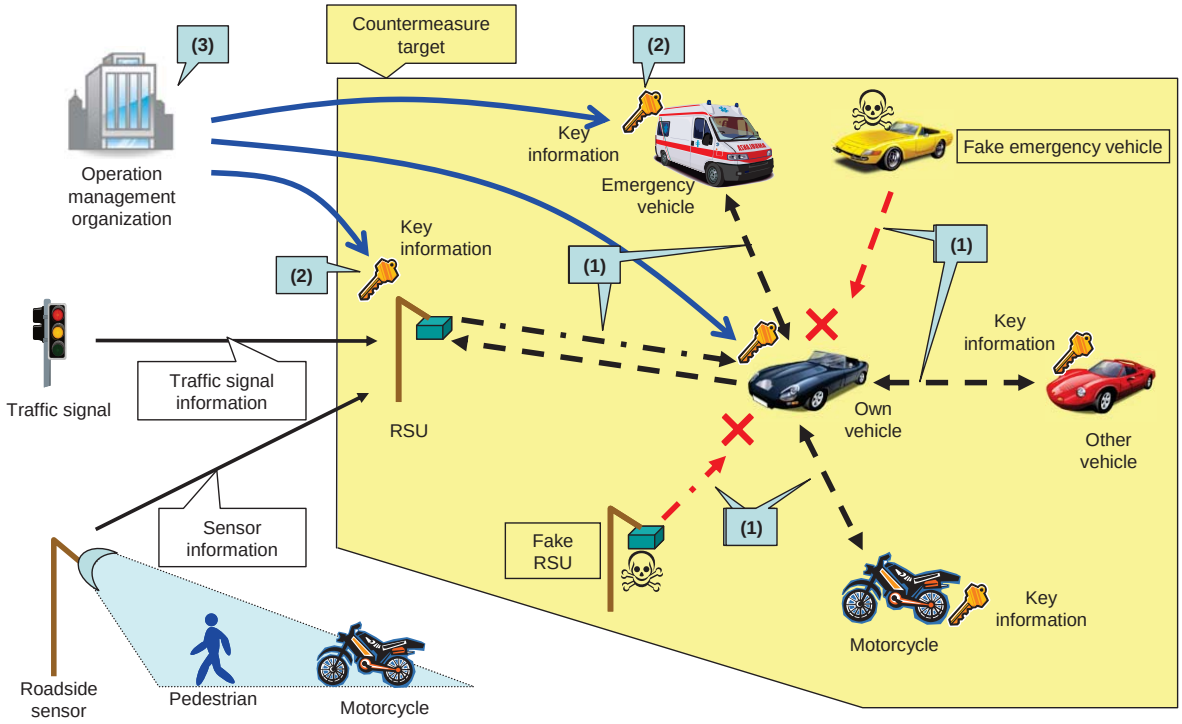


Figure 5-1: Security related countermeasure policy

[Blank]

Chapter 6: Security Measures

This chapter describes security measures for inter-vehicle and roadside-to-vehicle communication, security measures for communication equipment such as OBE and RSUs, and security measures for operation including systems on the infrastructure side.

6.1 Security measures for inter-vehicle and roadside-to-vehicle communication

This section describes methods for verifying the authenticity of the sender using encryption technology, for verifying message integrity, and for maintaining confidentiality of the communication information.

6.1.1 Verifying authenticity and integrity

Possible methods for verifying authenticity and integrity include the application of a digital signature using a public key algorithm (subsequently called digital signature method) or the use of a message authentication code (MAC) with a shared key algorithm (subsequently called MAC method). These are explained below.

6.1.1.1 Digital signature method

A security standard for inter-vehicle and roadside-to-vehicle communication is IEEE 1609.2 which is currently under deliberation in the U.S (see reference [8]). Under the viewpoint of international cooperation, adopting IEEE 1609.2 as the security standard for this driver assistance communications system is desirable. A signed message as defined in IEEE 1609.2 implements the application of a digital signature with a public key algorithm. The security measures for verifying the authenticity of the sender and the integrity of the message as mentioned in section 4.5 are covered by IEEE 1609.2. The following explanation is based on this method:

(1) Outline

At the receiving end, the method involves checking of a digital signature assigned to the message, and checking of a public key certificate issued by the sender, in order to implement authenticity and integrity verification. An outline of this method is shown in Figure 6-1.

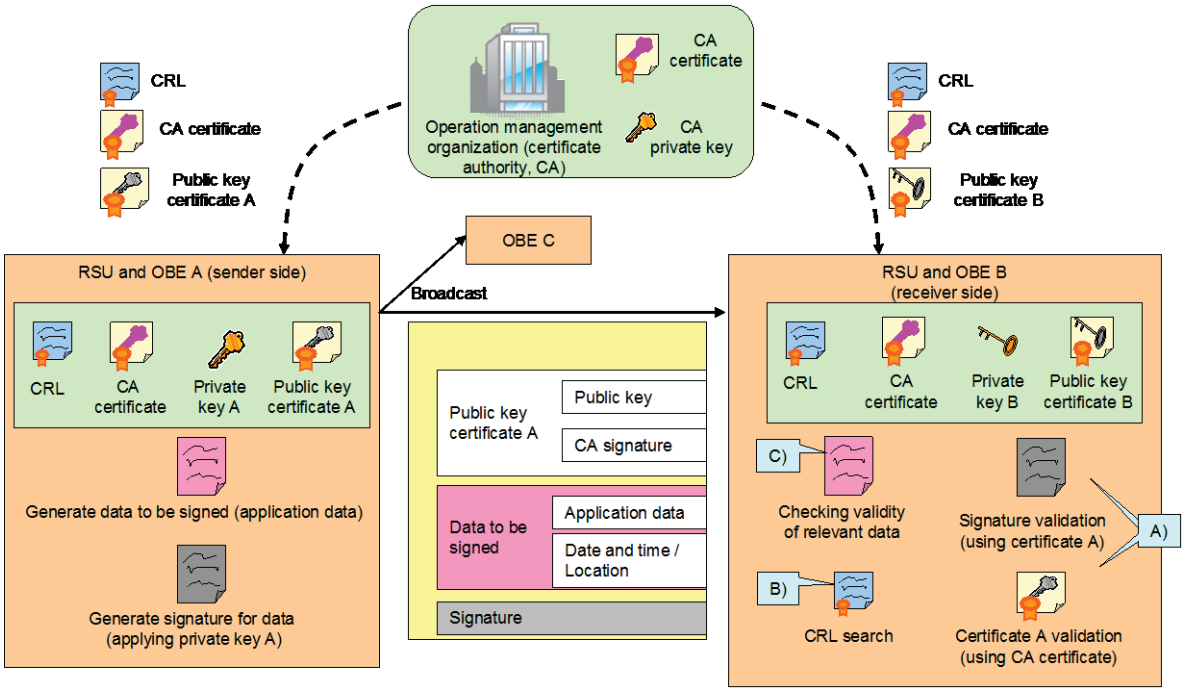


Figure 6-1: Outline of digital signature method

This method is an application of PKI (public key infrastructure). The OBE and RSU have both a unique private (secret) key for communication and a public key certificate. In operation, the sender and the receiver use different keys (private key and public key). The public key certificate serves to certify the owner of the public key matching the private key. It is issued by a trusted third party (CA: Certification Authority) using a digital signature that allows unique identification of the equipment to which it has been issued. In the driver assistance communications system, the CA is envisioned to be a private CA, namely the security information management section of the operation management organization. Having a CA with a hierarchical structure is also a possible approach. In this case, multiple CA certificates would exist, which would also have to be implemented in the equipment.

The sender uses its private key to generate a digital signature for the application data and other information to be broadcast (for OBE this includes drive information and general purpose information, for RSUs it is road information). The application data are then broadcast, along with the generated signature and the public key certificate, etc.

The receiver performs the following processing operations for the received message:

A) Verification of message authenticity and integrity

Public key certificate verification (verifying the CA signature by means of the CA public key

in the CA certificate), and digital signature verification of the application data (using the public key in the public key certificate) are performed. This makes it possible to verify that the received application data were sent by a party using the correct public key certificate, that the data were not tampered with, and that the sender is the owner of the public key certificate.

B) Negative list search

This involves checking to make sure that the received public key certificate is not included in the Certification Revocation List (CRL). In IEEE 1609.2, the public key certificate digest (certificate hash values) is included in this list which makes it possible to verify that the certificate is valid and has not been revoked (due to a security breach involving the private key or similar). The CRL includes a CA digital signature, which allows the use of the CA certificate to verify that the list has not been tampered with and that the issuer of the CRL is the CA.

Another possible method for implementing negative list search is the use of an Online Certificate Status Protocol (OCSP) to check the validity of the certificate. The OCSP approach is effective when the CRL has become too big, possibly causing problems with network bandwidth and insufficient equipment memory, provided that the equipment and the certificate authority are in constant communication contact. For example, the RSU must always be connected to the certificate authority and also must check the validity of the certificate of OBE, but if the number of cars with revoked certification has become large, using OCSP which involves only sending the serial number of the OBE certificate to the certificate authority and obtaining the checking result from the authority may reduce the memory requirements for the RSU.

C) Message validity verification

This involves verifying the date/time and position information included in a message, to make sure that application data are new (detection of resent data) and are geographically valid.

(2) Storing of security information

The unique private key and public key certificate must be stored in OBE and RSUs beforehand. The public key certificate requires the digital signature of the CA, and to generate the signature, the CA private key is used. The private key also is required to maintain confidentiality. The following two methods are possible for pre-storing of this information:

1. Generate a public key pair (matched private key and public key) in each equipment (OBE and RSU) and send the public key to the CA. The CA generates a public key certificate that is stored in each equipment.

2. The CA generates a public key pair and generates a public key certificate from the public key. The private key and the public key certificate are stored in each equipment.

Under the aspect of maintaining confidentiality, the private key does not leave each equipment when using method 1 and therefore no special measure is required. In the case of method 2, however, the private key generated by the CA has to be stored in each equipment, which means that measures to ensure confidentiality are required. On the other hand, method 1 requires that each equipment has the capability to generate a public key pair, while this capability is only required of the CA with method 2. Regardless of which of the above methods is used, linking of the private key and public key certificate to the equipment is necessary.

Besides the public key pair specific to each equipment, the CA certificate of each equipment and the CRL must also be stored in each equipment. For these, maintaining confidentiality is not required, but integrity must be assured. For the CA certificate and CRL, digital signing with the CA public key in the CA certificate can be used to verify integrity.

As described above, the CA certificate is a special kind of information that serves to verify other information. Tampering can be detected as described, but not swapping with a fake CA certificate. Therefore a means of properly storing the information in each equipment before operation is required.

(3) Updating security information

With this method, the following updates are required: private key and public key certificate of each equipment, CA certificate stored in each equipment, CRL.

Updating of the private key and public key certificate of each equipment can be done with the same methods as for pre-storing, as described above. For storing of information in equipment, updating by dealers, etc. or updating through RSUs are possible approaches. The required elements for updating are verification that the update request comes from genuine equipment, countermeasures against tampering and leaks (when including private key) in the communication channel between equipment and CA, and linking of update information (new certificate, etc.) to matching equipment.

Updating of the CA certificate stored in each equipment does not have a confidentiality requirement. Integrity can be verified as described above. Each equipment must be capable of verifying that the CA certificate has been issued by a genuine CA.

With regard to CRL updating, each equipment can perform tampering detection as described above and use the CA certificate to verify that the list has been issued by a genuine CA. However, the updated list must swiftly be distributed to each equipment.

(4) Communication format example

The communication format example of IEEE 1609.2 is shown below. The length of security related data (security data) is 196 bytes (excluding application data).

IEEE 1609.2 also includes various options, but the example shown below is a format where the data length has been kept as short as possible. In the illustration, figures in brackets indicate length, and "B" stands for Byte. The range covered by the digital signature is application data and security data such as date/time information.

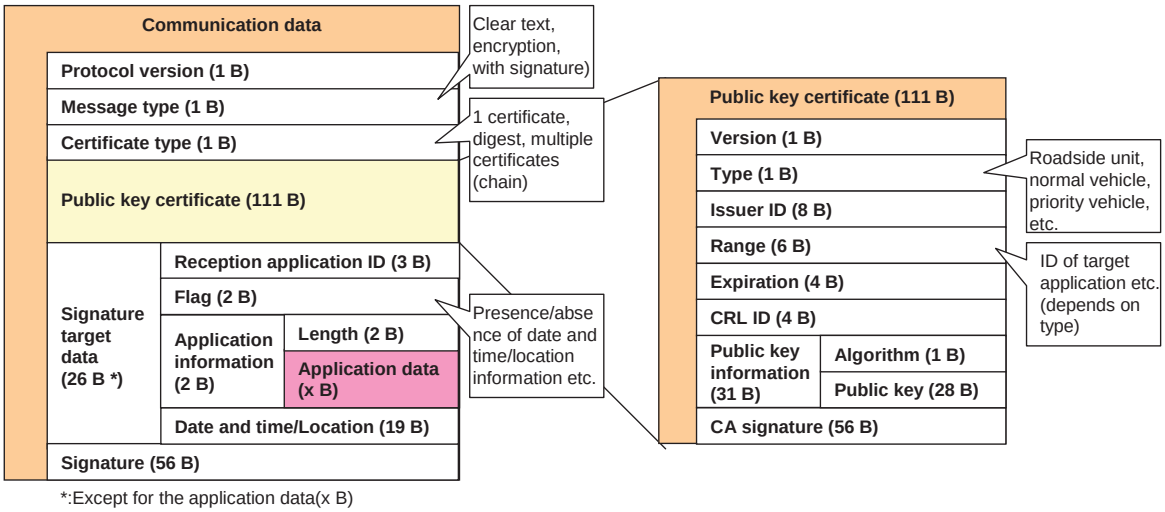


Figure 6-2: Communication format for digital signature method (IEEE 1609.2)

The table below lists information used for the digital signature method. In the confidentiality and integrity columns, ○ means required and X means not required.

Table 6-1: Information used for digital signature method

Information	Issue source	Storage location	Time used	Confidentiality	Integrity	Remarks
CA private key	CA	CA	・ Certificate issue ・ CRL issue	○	○	If this key is leaked, the entire system is at risk.
CA public key certificate	CA	(CA) Each equipment	・ Verification of public key certificate received from other equipment ・ Verification of received CRL	×	○	CA public key, etc. signed with CA private key
Private key of each equipment	① Each equipment ② CA	Each equipment	Signature generation for sending message	○	○	If this key is leaked, the respective equipment is at risk.

Information	Issue source	Storage location	Time used	Confidentiality	Integrity	Remarks
Public key certificate of each equipment	CA	(CA) Each equipment	Signature verification of message received from other equipment	×	○	・ Public key of equipment, etc. signed with CA private key ・ In case of ①, CA issues certificate based on public key generated by equipment
CRL	CA	(CA) Each equipment	Receiving message from other equipment	×	○	Digest list of certificates revoked within expiration period (lower 10 bytes of certificate hash value), signed with CA private key

6.1.1.2 MAC method

Compared to using a public key algorithm, the use of a shared key algorithm reduces the processing load. This method therefore can be implemented also on equipment with less processing power, given the same timeframe. However, the shared key algorithm requires that the same key is used at the sending side and the receiving side. When an unspecified number of multiple devices are used, the entire system must perform communication using one key (see Annex A). Consequently, if this key was leaked at a single location, the key information at all devices must be renewed. Also, because specific equipment cannot be determined from its key, allocation of equipment IDs is necessary for this purpose. When implementing measures to prevent spoofing, it must be assumed that the equipment ID stored in the equipment has not been modified.

(1) Outline

The use of a shared key algorithm may be implemented either through encryption or with a MAC. The former is aimed mainly at maintaining confidentiality and the latter at integrity and authenticity. In this guideline, the targets are authenticity and integrity, therefore the MAC principle is applied.

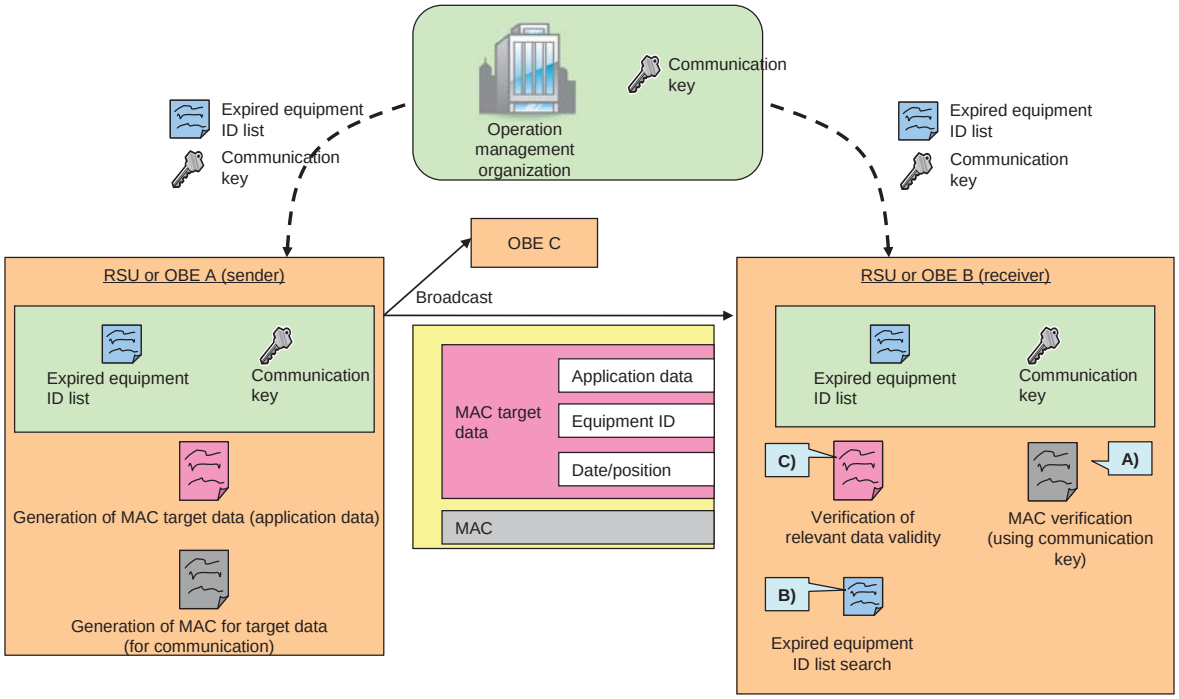


Figure 6-3: Outline of MAC method

With this method, the OBE and RSU use a shared key for communication. The same key is used at the sending side and the receiving side.

The sender uses the communication key to generate a MAC for the application data and equipment ID information, etc. to be broadcast (for OBE this includes drive information and general purpose information, for RSUs it is road information). The application data are then sent along with the generated MAC and equipment ID, etc.

The receiver performs the following processing operations for the received data:

A) Verification of message authenticity and integrity

Verification of MAC for the application data (generating a MAC for the application data using the communication key and comparing it to the received MAC) is performed. This allows checking that the sender of the received application data possesses the genuine communication key and that the application data were not tampered with.

B) Negative list search

Checking is performed to verify that the received equipment ID is not included in the list of expired equipment IDs (expired equipment ID list). This ascertains that the sender equipment is not expired.

C) Message validity verification

This involves verifying the date/time and position information included in a message, to make

sure that application data are new (detection of resent data) and are geographically valid.

(2) Storing of security information

The communication key must be stored in the OBE and RSUs beforehand, and confidentiality of the communication key must be maintained. Consequently, the communication key issued by the operation management organization must be stored in each equipment in such a way that confidentiality is not compromised. Because the same communication key is used for all equipment with the MAC method, the key stored in all devices must be updated if the communication key has been leaked.

Besides the communication key, the expired equipment ID list must also be stored in each equipment. The expired equipment ID list corresponds to the CRL in the digital signature method. Confidentiality is not required, but a means for verifying that the list has not been tampered with and is the genuine list issued by the operation management organization must be provided, to ensure authenticity and integrity.

(3) Updating security information

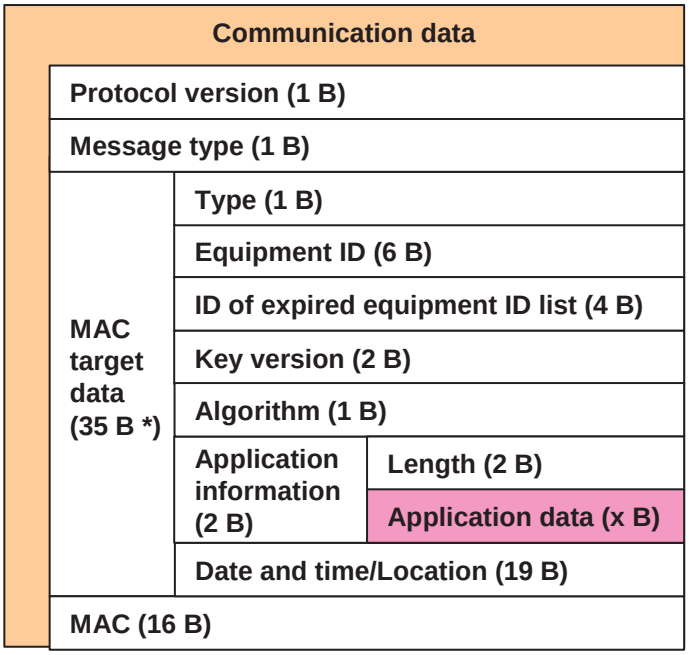
With this method, the following updates are required: communication key of each equipment, expired equipment ID list.

For updating the communication key, updating by dealers, etc. or updating through RSUs or telematics are possible approaches. Countermeasures against tampering and leaks in the route between equipment and the operation management organization must be implemented.

When updating the expired equipment ID list, tampering detection as above and checking that the list is the genuine list issued by the operation management organization must be implemented.

(4) Communication format example

An example for the communication format when using the MAC method is given below. In this example, the length of the security data is 53 bytes. This assumes that the type of sender information (indicating RSU, OBE, or other equipment) is 1 byte, and the equipment ID is 6 bytes. In the illustration, figures in brackets indicate length, and “B” stands for Byte. The range covered by the MAC is application data and security data such as date/time information, equipment ID, etc.



*:Except for the application data(x B)

Figure 6-4: Communication format example for MAC method

The table below lists information used for the MAC method. In the confidentiality and integrity columns, ○ means required and X means not required.

Table 6-2: Information used for the MAC method

Information	Issue source	Storage location	Time used	Confidentiality	Integrity	Remarks
Communication key	Operation management organization	(Operation management organization) Each equipment	・MAC generation for sending message ・MAC verification of message received from other equipment	○	○	If this key is leaked, the entire system is at risk.
Expired equipment ID list	Operation management organization	(Operation management organization) Each equipment	Receiving message from other equipment	×	○	Expired equipment ID list

6.1.1.3 Features of each method

The following table compares the features of the digital signature method and the MAC method:

Table 6-3: Features of each method (outline)

		Digital signature method	MAC method	Remarks
Method		Digital signature	MAC	—
Algorithm example (key length)		ECDSA (224 bit)	AES (128 bit)	—
Key information stored in each equipment *		・ CA public key certificate ・ Private key of respective OBE or RSU ・ Public key certificate of respective OBE or RSU	Communication key	* Does not include a key for securely storing or updating key information.
Key used for communication		Unique to respective OBE or RSU	Common for all OBE and RSUs	—
Processing at each equipment	When sending	Generate signature	Generate MAC	—
	When receiving	Verify signature (2 times*)	Generate and compare MAC	* One time if using verified certificate
Confidential information	OBE RSU	Private key of respective OBE or RSU	Communication key	—
	System	CA private key	Communication key	—
Revised information when updating		・ CA private key or public key certificate ・ Private key and public key certificate of respective OBE or RSU ・ CRL	・ Communication key ・ Expired equipment ID list	—
Security data length*		196 B	53 B	*See Figure 6-2 and Figure 6-4

Table 6-4: Features of each method (security)

		Digital signature method	MAC method
Normal state	Spoofing by third party	Because the third party will not possess a CA issued public key certificate, spoofing can be detected by public key certificate verification.	Because the third party will not know the communication key, spoofing can be detected by MAC verification.
	Spoofing of other equipment by user	Because private key of other equipment will not be known, spoofing can be detected by public key certificate verification and message signature verification.	Spoofing can be detected by MAC verification for equipment ID. (provided that stored equipment ID has not been falsified)
	Falsification of equipment output data	Can be detected by message signature verification.	Can be detected by message MAC verification .
	Falsification of data stored in equipment (key information or equipment ID, type information)	Can be detected by public key certificate verification and message signature verification.	Cannot be detected.
	Falsification of external input data	No countermeasure	No countermeasure
	Equipment identification	Identification possible by public key certificate	Identification possible by equipment ID (provided that stored equipment ID has not been falsified)
	Replay attack	Can be detected by checking date and time or location information, etc.	Can be detected by checking date and time or location information, etc.
When communication key has been leaked	Spoofing of other equipment	Spoofing by equipment other than the one with the leak is not possible. (detection via CRL possible)	Spoofing of other equipment is possible, because a message can be generated with any equipment ID.
	Identification of equipment where leak occurred	Identification possible by public key certificate	Identification not possible

		Digital signature method	MAC method
	Countermeasure when private key, etc. of specific equipment has been leaked	・ Updating of private key and public key certificate of specific equipment ・ CRL updating	Updating of communication key used by all OBE and RSUs
	Prevention of leak re-occurrence	Because equipment with leak can be identified, prevention is possible.	Because equipment with leak cannot be identified, re-occurrence is possible.
Negative list		Digest list of public key certificates (partial hash values of certificates) (CRL)	List of IDs of expired equipment (expired equipment ID list)
	Falsification	Can be detected by signature verification of CA certificate.	Separate framework for detecting falsification is necessary.
	Delayed risk (negative list update)	Until updated CRL is received, use of expired public key certificate is possible.	Until updated expired equipment ID list is received, use of expired equipment is possible.

Table 6-5 Features of each method (cost)

		Digital signature method	MAC method	Remarks
Registration step		Medium (Offline certificate issue)	Low (Offline communication key issue)	—
	Required procedures	・ Issuing of public key certificate for each equipment ・ Issuing of CA certificate ・ Issuing of CRL	・ Issuing of common communication key ・ Issuing of expired equipment ID list	—
Regular maintenance		High (Offline CRL updating)	High (Online updating of expired equipment ID list)	—
	Required procedures	・ Updating of key pair and certificate for each equipment ・ Updating of CA certificate ・ Updating of CRL	・ Updating of communication key ・ Updating of expired equipment ID list	—
Crisis management in case of key information leak		Low (Only affected equipment)	High (All OBE and RSUs)	—
	Required procedures	・ Updating of leaked private key ・ Updating of CRL	Updating of communication key	—
Processing power and scale requirements at each equipment		High	Low	Digital signature method with public key algorithm causes a higher processing load than MAC method with shared key algorithm.
Implementation of tamper resistance	Requirements	Medium (Protection of private key of each equipment)	High (Protection of communication key for entire system)	—
	Purpose	Confidentiality of private key	・ Confidentiality of communication key ・ Integrity of equipment ID and type information must be ensured	—

6.1.2 Method for maintaining confidentiality of communication information

A method for maintaining confidentiality is the use of encryption with a shared key algorithm.

Various modes for encryption exist. The CTR (Counter) mode which yields a constant encryption result length, or stream encryption are considered suitable. Because the encryption processing result would be the same for the same data, unless the encryption key and other parameters were changed, “nonce” (a variable not used repeatedly with the same key) is used to ensure a different encryption processing result also when encrypting the same data with the same key. Since data integrity cannot be assured simply by using encryption, it should be combined with the digital signature method or MAC method described in the preceding sections. When a shared key algorithm is used, the key used for encryption will have to be transmitted in communication for the entire system as a single key, as described in section 6.1.1.2 (see Annex A).

The purpose of maintaining confidentiality, as described in chapter 4, is to prevent eavesdropping and misuse of messages for services other than those for which the system is designed. The target range for encryption therefore encompasses application data and security data (except for key IDs and other data that need to be in clear text).

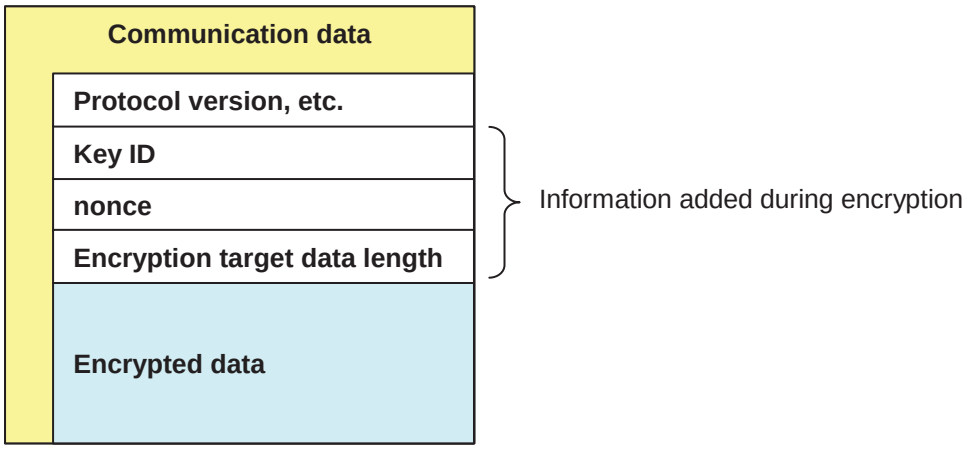


Figure 6-5: Example for encryption using nonce

IEEE 1609.2 [8] also defines a method for maintaining confidentiality using both a public key algorithm and a shared key algorithm. A shared key generated at the sender side is used to encrypt the data to be protected, and this shared key is then encrypted using the public key of the receiver. Consequently, this method can be used only when the sending target (receiver) is known. However, maintaining confidentiality in the current system requires protecting the communication data from eavesdropping by a third party (not using genuine equipment), and in this system data are distributed to all genuine equipment. The shared key encryption method of

IEEE 1609.2 is therefore no suitable.

6.1.3 Encryption algorithm

The encryption algorithm is to be chosen from the CRYPTREC* list of recommended cryptographic techniques for government and industrial use. Information about risks involving the encryption algorithm selected for the system should also be collected as required. If the algorithm has been compromised, key length and algorithm selection must be reviewed.

* Cryptography Research and Evaluation Committees in Japan

6.2 Security measures in RSUs and OBE

6.2.1 Security information stored in RSUs and OBE

In order to maintain the security described in section 6.1, the following information must be stored in the RSUs and OBE, according to the respective requirements:

- Key information

In order to check integrity and maintain confidentiality of messages exchanged during inter-vehicle communication or roadside-to-vehicle communication, key information is required. Key information includes not only the keys used in actual inter-vehicle communication or roadside-to-vehicle communication, but also keys used for secure initial registration or updating of communication keys in RSUs or OBE, keys for verifying that the negative list described below is genuine, etc. Details if the key information will depend on the encryption method used.

- Type information

Type information that distinguishes for example between a RSU, OBE for ordinary vehicles, and OBE for priority vehicles is necessary as a countermeasure against spoofing whereby a sender masquerades as a RSU or OBE by giving false sender information.

- Equipment ID

An equipment ID is necessary in order to uniquely identify a modified RSU or OBE.

- Date and time information

In order to guard against a replay attack where the send timing is modified, a means of indicating the send date and time of each message is required (see Annex B).

- Location information

In order to guard against a replay attack where the send location is modified, a means of indicating the send location of each message is required.

- Negative list

In order to allow the receiving RSU or OBE to eliminate messages from a modified RSU or OBE, a negative list is required.

6.2.2 Manufacture of RSUs and OBE

The function module in the RSU or OBE for handling security information must be manufactured in a managed environment designed to prevent security information leaks or modification.

6.2.3 Deployment of RSUs and OBE

As shipped from the factory, the function module in the RSU or OBE for handling security information must include the following countermeasures against tampering:

- Analysis of processes related to security information must be difficult.
- Key information except for the public key must not be readable or extractable from outside.
- Except when using equipment and/or technology designed for the purpose of updating security information, it must not be possible to modify security information or modify or disable security information related processing.

6.3 Security measures at operation management organization

This section deals with security measures at the operation management organization, divided into measures with regard to external entities such as equipment manufacturers, and internal measures.

6.3.1 Security measures with regard to external entities

Security measures related to external entities are described below, divided into measures for the development and manufacturing phase of OBE and RSUs, measures for the installation and marketing phase, and measures for the operation phase.

6.3.1.1 Development and manufacturing phase

In the development and manufacturing phase of OBE and RSUs, security specifications and test key information for use in testing must be provided to the manufacturer.

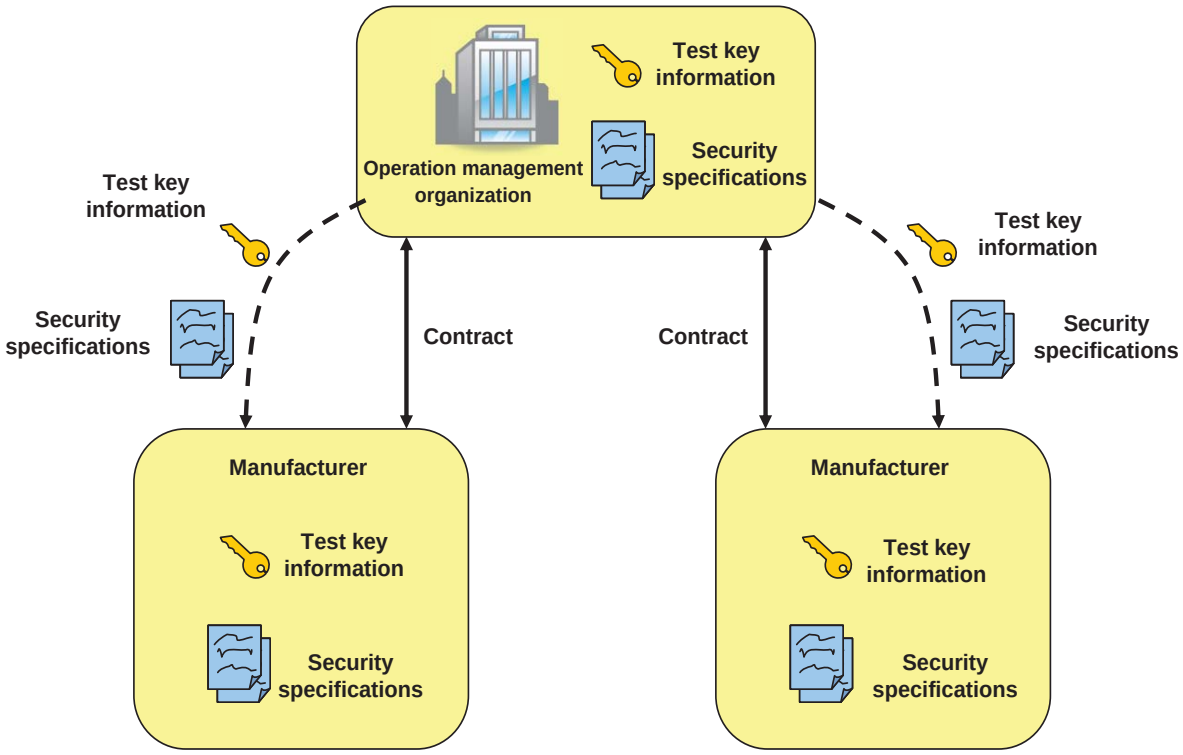


Figure 6-6: Development and manufacturing phase

When the operation management organization provides security specifications and test key information on a leasing basis, recipients must first be screened and a contract must be concluded. The operation management organization shall have the recipients bear the obiligation of confidentiality of seculity information (the security specifications, test key information, etc), and also during the handing-over stage. Manufacturers who do not further use this information should be required to return the information provided on a leasing basis.

6.3.1.2 Installation and marketing phase

In the installation and marketing phase, key information and an initial negative list are provided and stored in the respective equipment, as shown in Figure 6-7.

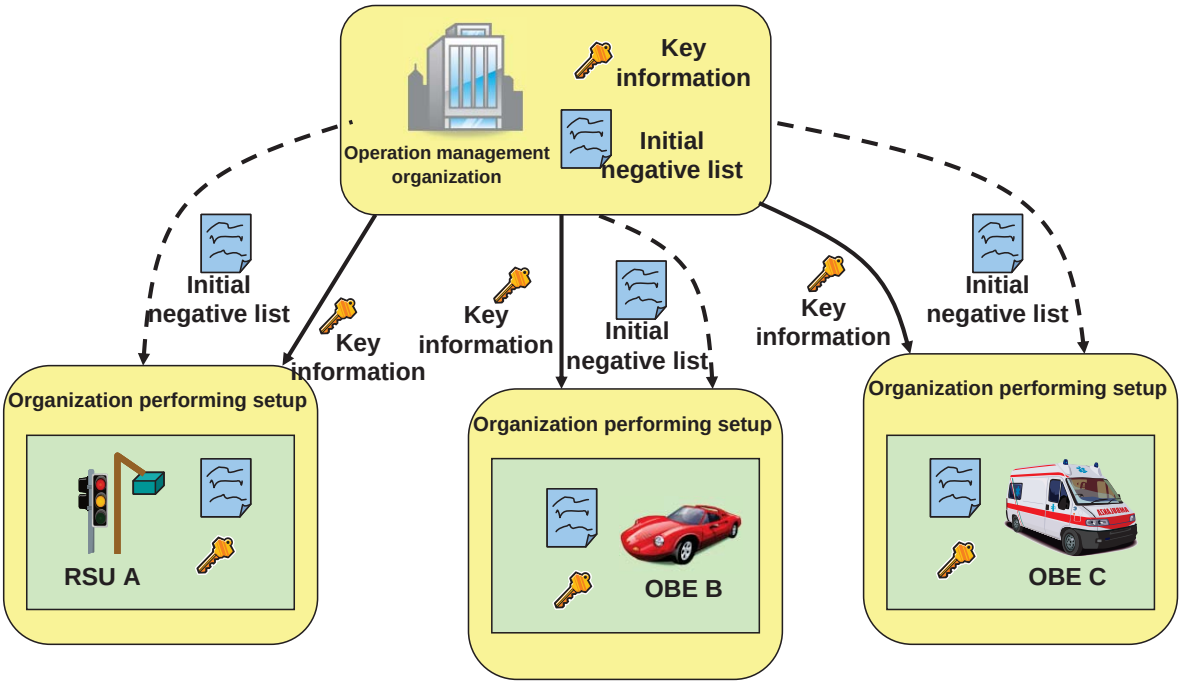


Figure 6-7: Installation and marketing phase

The key information to be stored in each equipment depends on the method, as described in section 6.1. The various items are listed in Table 6-6. Security measures are categorized with regard to confidentiality and integrity. The indication "(achieved)" means that the item is covered with the respective method. (For example, the public key certificate for each equipment can be verified with the CA public key certificate.) The private key for each equipment can be either (1) generated at the respective equipment, or (2) generated by the CA.

Table 6-6: Key information stored in each equipment

Purpose	Method	Key information	Required security measure
Authenticity check Integrity check	Digital signature	CA public key certificate	Integrity (achieved)
		Private key of each equipment	Confidentiality, integrity
		Public key certificate of each equipment	Integrity (achieved)
	MAC	Communication key	Confidentiality, integrity
Maintaining confidentiality	Encryption	Encryption key	Confidentiality, integrity

With the digital signature method, besides the above key information to be stored in each equipment, the CA private key generated at the operation management organization is also required, and its confidentiality and integrity must be ensured.

The requirements for the initial negative list are shown in Table 6-7. Because the CRL has a CA signature, its integrity can be verified using the CA certificate.

Table 6-7: Negative list stored in each equipment

Measure	Method	Negative list	Required security measure
Authenticity check	Digital signature	CRL	Integrity (achieved)
Integrity check	MAC	Expired equipment ID list	Integrity

The security measures required for the installation and marketing phase are described below:

- Management of CA private key at operation management organization (digital signature method)

If the CA private key has been leaked or falsified, third parties can issue a false public key certificate or false CRL, resulting in the need to change the public key certificate of all equipment. Therefore it is mandatory that confidentiality and integrity are maintained.

- Maintaining authenticity of operation management organization

If a third party pretends to be the operation management organization and distributes false CA certificates or communication keys, communication with equipment in which this false key information was stored will not be possible. Manufacturers receiving key information therefore must be able to ascertain the authenticity of the operation management organization to ensure that only genuine key information is being accepted. A suitable framework for this purpose must be established.

- Maintaining authenticity of equipment manufacturers receiving key information

If the operation management organization distributes key information to an unauthorized third party organization, there is a risk that the information may be used inappropriately. The operation management organization therefore must be able to ascertain the authenticity of the equipment manufacturer. A suitable method for this purpose must be implemented.

- Protection of communication channels between operation management organization and equipment manufacturers

In order to prevent leaking or falsification of key information carried in communication channels between the operation management organization and the equipment manufacturers, the confidentiality and integrity of the communication channels must be maintained. The

information required for maintaining confidentiality and the information required for maintaining integrity differ, depending on the method (see Tables 6-6 and 6-7).

- Maintaining confidentiality and integrity of key information at equipment manufacturers

If key information has been leaked from an equipment manufacturer or has been falsified at an equipment manufacturer, the key information can no longer be used. Consequently, the manufacturer needs to maintain confidentiality and integrity of key information received from the operation management organization. The information required for maintaining confidentiality and the information required for maintaining integrity differ, depending on the method (see Tables 6-6 and 6-7).

- Maintaining integrity of expired equipment ID list (MAC method)

If a false expired equipment ID list issued by a third party or a falsified list created by modifying a genuine list is stored in each equipment, normal communication will not be possible. Consequently, the integrity of the expired equipment ID list must be maintained.

6.3.1.3 Operation phase

As shown in Figure 6-8, the key information and negative list stored in each equipment will require updating.

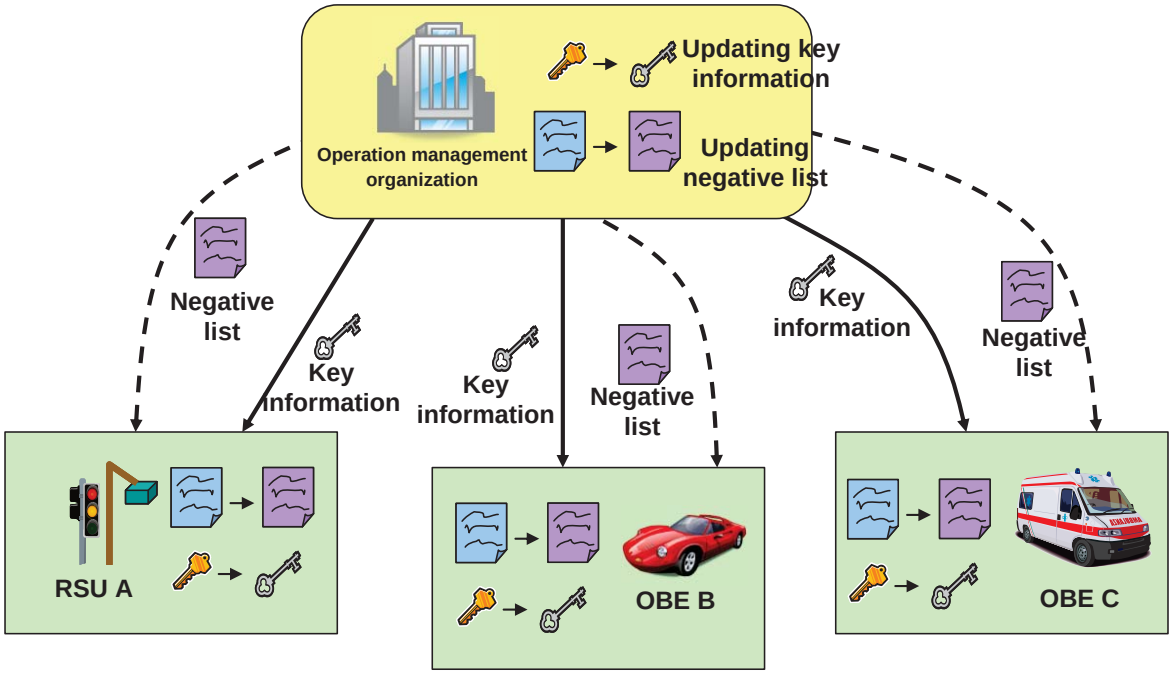


Figure 6-8: Operation phase

The key information to be stored in each equipment depends on the method, as described in section 6.1. The various items are listed in Table 6-8. With the digital signature method, the private key to be stored for each equipment can be either (1) generated at the respective equipment, or (2) generated by the CA.

Table 6-8: Key information requiring updating in each equipment

Purpose	Method	Key information	Required security measure
Authenticity check Integrity check	Digital signature	CA public key certificate	Integrity (achieved)
		Private key of each equipment	Confidentiality, integrity
		Public key certificate of each equipment	Integrity (achieved)
	MAC	Communication key	Confidentiality, integrity
Maintaining confidentiality	Encryption	Encryption key	Confidentiality, integrity

With the digital signature method, besides the above key information for each equipment, the CA private key updated at the operation management organization is also required, and its confidentiality and integrity must be ensured.

The requirements for the negative list are shown in Table 6-9.

Table 6-9: Negative list update requirements for each equipment

Measure	Method	Negative list	Required security measure
Authenticity check	Digital signature	CRL	Integrity (achieved)
Integrity check	MAC	Expired equipment ID list	Integrity

The security measures required in the operation phase are listed below:

- Management of CA private key at operation management organization (digital signature method)

As in the marketing and installation phase, if the CA private key has been leaked or falsified, third parties can issue a false public key certificate or false CRL, resulting in the need to change the public key certificate of all equipment. Therefore it is mandatory that confidentiality and integrity of the CA private key are maintained.

- Maintaining authenticity of operation management organization

If a third party pretends to be the operation management organization and distributes false CA certificates or communication keys to OBE or RSUs, communication with equipment in which this false key information was stored will not be possible. Therefore a method that allows checking that the key information or negative list was issued by the genuine operation management organization must be implemented in OBE and RSUs.

- Maintaining authenticity of equipment where key information is being updated

If an update request from unauthorized equipment causes the operation management organization to distribute key information to that equipment, there is a risk that the key information will be misused. Therefore the operation management organization needs to verify that equipment is genuine.

- Protection of communication channels between operation management organization and equipment

In order to prevent leaking or falsification of key information carried in communication channels between the operation management organization and the equipment, the confidentiality and integrity of the communication channels must be maintained. The information required for maintaining confidentiality and the information required for maintaining integrity differ, depending on the method (see Tables 6-8 and 6-9).

- Maintaining integrity of expired equipment ID list (MAC method)

If an expired equipment ID list issued by a third party or a falsified list created by modifying a genuine list is used for updating each equipment, normal communication will not be possible. Consequently, the integrity of the expired equipment ID list must be maintained.

6.3.2 Internal security measures at operation management organization

As shown in Figure 6-9, the operation management organization must securely manage key information and negative list information used by the system.

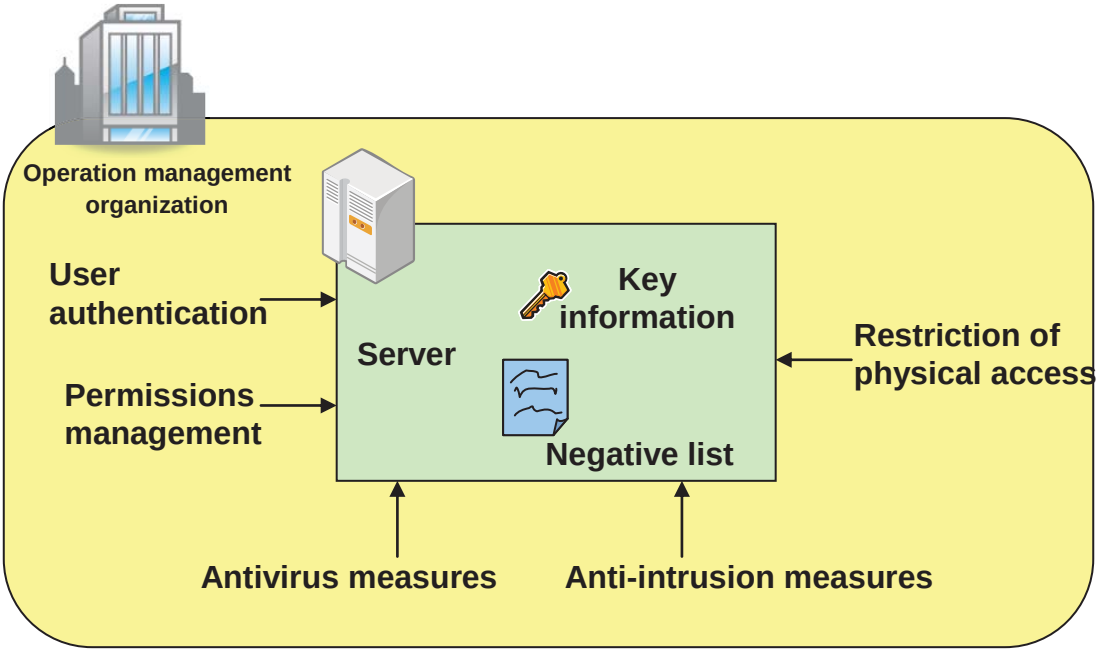


Figure 6-9: Internal security measures at operation management organization

Servers at the operation management organization used for issuing and managing key information and negative list information must be protected against unauthorized external access, as well as against viruses and other risks. Measures for authentication of server users and measures for proper access permissions management must also be in place. In particular, key information (such as the CA private key, communication key, etc.) must be strictly protected, because key information in every equipment of the system must be changed if such information is leaked or compromised. Using tamper-proof hardware security modules for handling key information is desirable. The installation environment also must allow for restricting physical access to servers.

[Blank]

Chapter 7: Appendix

Annex A. Key management when using a shared key algorithm

Systems using a shared key algorithm generally require a transaction where the session key (shared key) is shared using a previously stored store key (shared key) prior to actual data exchange. The session key is a disposable key used only for that communication session (encrypting data with the same key over longer periods incurs a security risk).

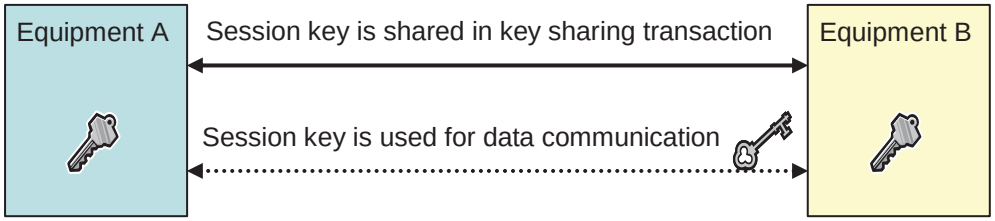


Figure 7-1: General shared key type system

Consequently, a parent equipment device (A) communicating with multiple equipment devices (B, C) must have multiple store keys (as many as there are devices).

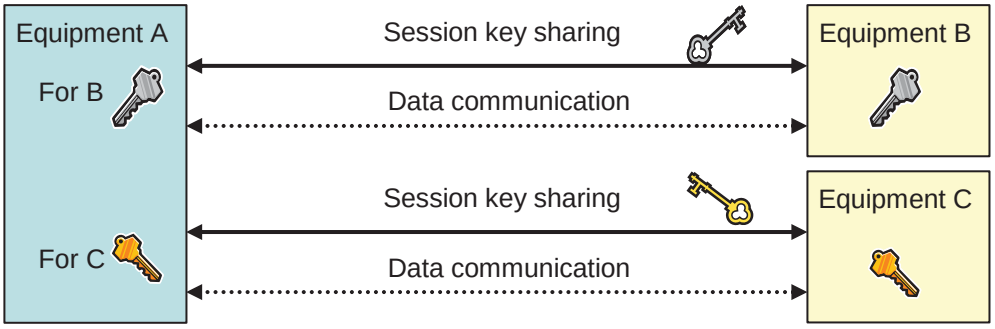


Figure 7-2: Communication with multiple equipment devices

On the other hand, in inter-vehicle communication all OBE devices become parent devices, and would have to possess as many store keys as there are other OBE devices.

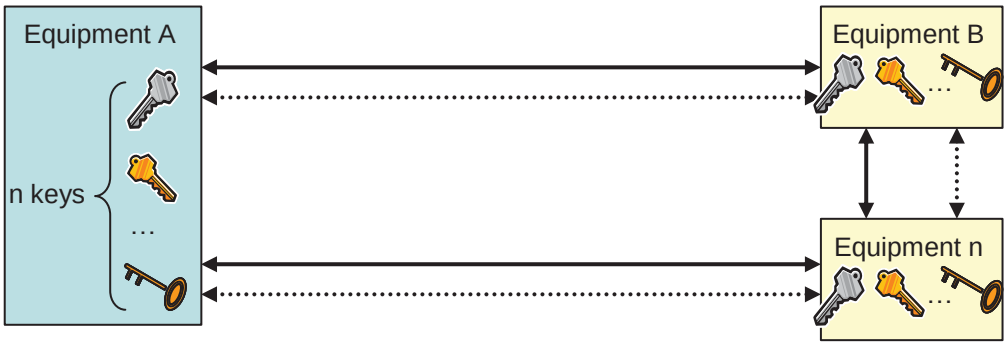


Figure 7-3: Inter-vehicle communication (1)

In practice, possessing store keys for all OBE devices is not possible, and a key sharing transaction for broadcast communication is also not feasible. Consequently, inter-vehicle communication can only be realized by using a single system-wide key (the same shared key is stored in all OBE devices).

Figure 7-4: Inter-vehicle communication (2)

Annex B. Replay attacks

Handling of date/time data and detection of replay attacks

3. No counter value based countermeasures, no date/time data
   - Attacker can use any send timing and can attack any send target.
     (Attacker could accumulate for example received sudden braking data and send sudden braking information for a non-existent vehicle in order to create confusion, which could even stop an emergency vehicle. This may lead to serious accidents.)
4. Counter value based countermeasures, no date/time data
   - A counter value incremented with every send operation or similar is used, unrelated to date and time.
   - In order to verify the counter, the OBE must have saved information about the send source ID and the latest counter value.
   - By comparing the received message to these data, it is possible to determine whether the received message is a resend of an already received message or a resend of an earlier message (within the saved range).
   - Resend detection for previously non-received messages or later messages is not possible.

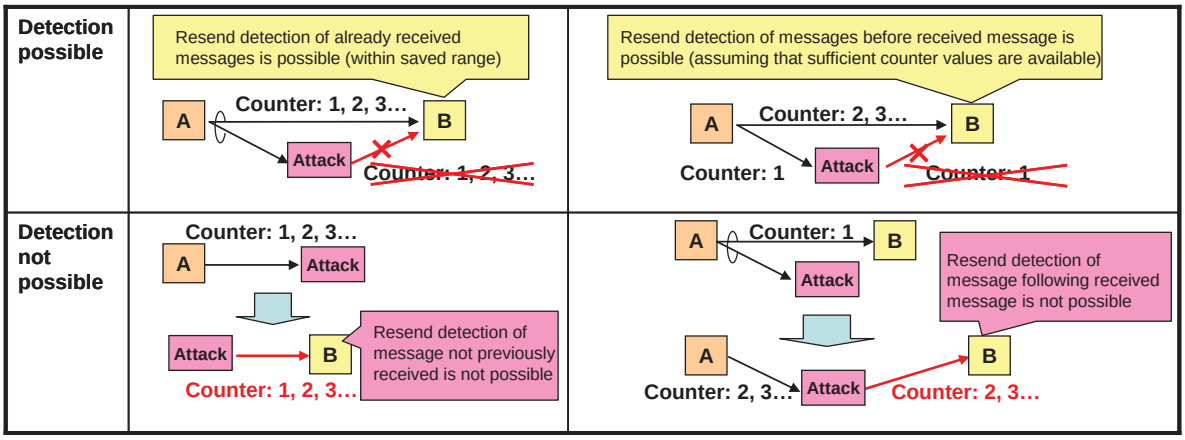


Figure 7-5: Counter value based countermeasures, no date / time data

5. No counter value based countermeasures, time data (h/m/s) present
   - Because there are no date data, resend attack on subsequent days at the same time cannot be detected.

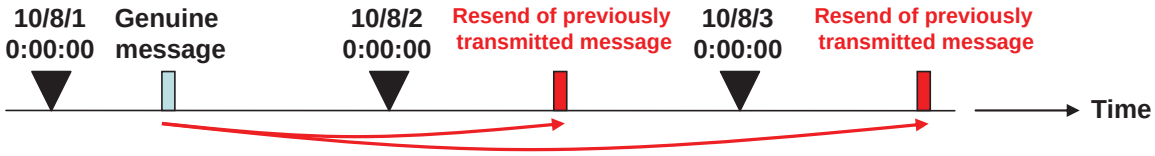


Figure 7-6: Replay attack at same time on subsequent days

- Resend attack in increments of less than or equal to one second cannot be detected.

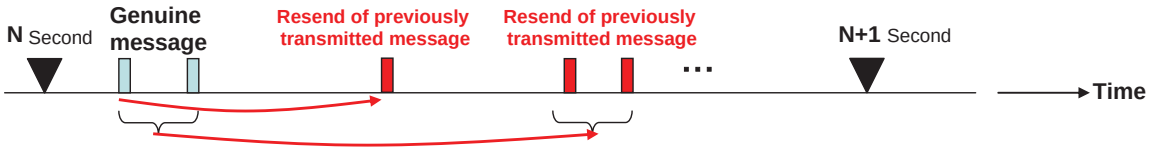


Figure 7-7: Replay attack using less than or equal to one second units

6. Counter value based countermeasures, time data (h/m/s) present
   - Because there are no date data, resend attack on subsequent days at the same time cannot be detected.
   - Adding counter values to time data (h/m/s) allows detecting resend attacks in increments of less than or equal to one second.
   - For messages resent in increments of less than or equal to one second, comparison to the received message makes it possible to determine whether the received message is a resend of an already received message or a resend of an earlier message. (Because it is necessary to save the sending OBE ID and the latest counter value, detection is possible only within the saved range.)
   - Detection of resend in increments of less than or equal to one second for previously non-received messages or later messages is not possible.
7. No counter value based countermeasures, date/time data (yyyy/mm/dd/h/m/s) present
   - Resend attack in increments of less than or equal to one second cannot be detected.
8. Counter value based countermeasures, date/time data (yyyy/mm/dd/h/m/s) present
   - Adding counter values to date/time data (yyyy/mm/dd/h/m/s) allows detecting resend attacks in increments of less than or equal to one second.
   - For messages resent in increments of less than or equal to one second, comparison to the received message makes it possible to determine whether the received message is a

resend of an already received message or a resend of an earlier message. (Because it is necessary to save the sending OBE ID and the latest counter value, detection is possible only within the saved range.)

- Detection of resend in increments of less than or equal to one second for previously non-received messages or later messages is not possible.

Annex C. Examples of attacks on road information (indirect)

Counter-measure	Attack 1 Send time falsification	Attack 2 Roadside-to-vehicle communication time falsification	Attack 3 Roadside-to-vehicle communication time forgery	Cost	Influence on communication specifications	Advantages	Disadvantages
1. Regulating the transmission count	△ (○ if no forward transmissions)	△	×	○	○	・ Easy to implement	・ Reduced communication success rate of roadside-to-vehicle communication in areas where attackers operate
2. Conflict detection before inter-vehicle communication	○ (*1)	○ (*1)	○ (*1)	○	Details to be worked out	・ Suppression of attacks directed at inter -vehicle communication possible ・ Influence only in areas where attackers operate ・ Influence of setting mistakes in RSUs can be reduced	・ Communication success rate of roadside-to-vehicle communication in areas where attackers operate reduced to level of inter-vehicle communication
3. Encryption of road information (indirect)	○	○	○	×	×	・ Entire road information (indirect) can be protected	・ Large influence on communication specifications ・ High cost
4. Regulating the service level (*2)	△	△	△ (○ if combined with countermeasure 2)	○	○	・ Control of roadside-to-vehicle communication time forgery possible	・ Regulating rate of roadside-to-vehicle communication time required ・ inter-vehicle communication service is assumed to coexist with roadside-to-vehicle communication service

*1 Communication period for inter-vehicle communication can be ensured even if attackers exist

*2 Adjust service level to fulfill the following two points:

・ Regulate rate (maximum value) of roadside-to-vehicle communication time

・Inter-vehicle communication service is assumed to coexist with roadside-to-vehicle communication

Annex D. Considering primitives for storing/updating/changing security information

Besides the primitives for controlling security processing in inter-vehicle and roadside-to-vehicle communication, primitives must also be set for security control tasks required for system operation, such as storing and updating security information, changing security settings, etc.

Examples for primitives required for security control, including storing and updating keys as security information, obtaining security information, and changing settings are given below, along with sample procedures for security control.

1. Primitives required for security control (example)

The primitives shown below can be used to control the security section of the equipment.

・**SecurityCont.Request(** Security Control Information, Security Control Data Length, Security Control Data)	・**SecurityCont.Response(** Security Control Information, Security Control Data Length, Security Control Data)

(Security Control Information: information related to security processing block, length 1 byte)
(Security Control Data Length: length of security control data, length 2 bytes)
(Security Control Data: security control data, length as specified by Security Control Data Length)

<Reference> Primitives and processing flow for security control in communication (example)

Security processing flow with [Security.Request, Security.Response, Unsecurity.Request, Unsecurity.Response]

・Status of security flag in L7 layer determines security processing

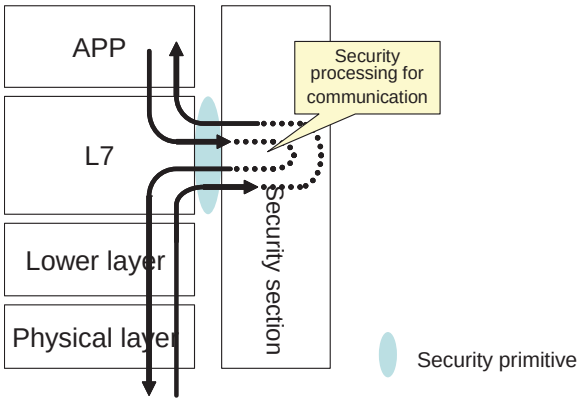


Figure 7-8: Processing flow for security control in communication (example)

2. Security control procedure (example)

a) System control section using external interface for security control

As shown in the illustration below, an external interface (such as an IC card reader, USB port, serial port, etc.) connected to the equipment is used, and the system control section manages input/output of information required for security control (new security information, update data, security setting change instructions, etc. The following steps are executed:

① The security control data are input via the external interface physically connected to the system control section of equipment.

② The security control data are received by the system control section.

③ The security control data are analyzed and evaluated by the system control section.

④ The security control data are passed on to the security section as required. (Primitive: SecurityCont.Request)

⑤ The security section performs control processing according to the input security control data.

⑥ The security section returns the processing results to the system control section. (Primitive: SecurityCont.Response)

In this case, a security control primitive must be placed between the system control section and the security section.

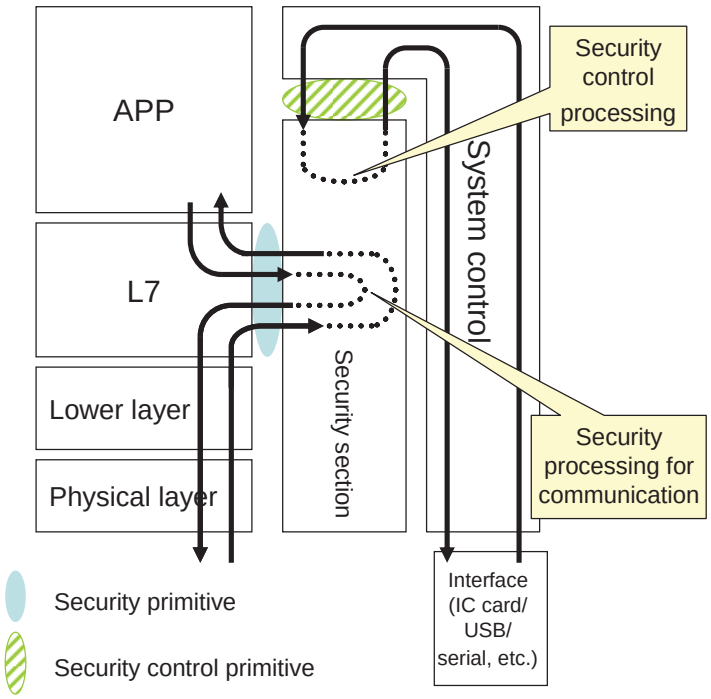


Figure 7-9: System control section using external interface for security control

b) Security control application using external interface for security control

As shown in the illustration below, an external interface connected to the equipment is used, and the security control application manages input/output of information required for security control. The following steps are executed.

① The security control data are input via the external interface physically connected to the system control section of equipment.

② The security control data are received by the system control section.

③ The system control section passes the security control data to the security control application.

④ The security control data are analyzed and evaluated by the security control application.

⑤ The security control data are passed on by the security control application to the security section as required. (Primitive: SecurityCont.Request)

⑥ The security section performs control processing according to the input security control data.

⑦ The security section returns the processing results to the security control application. (Primitive: SecurityCont.Response)

⑧ The security control application passes the processing result data etc. to the system control section as required.

In this case, a security control primitive must be placed between the application layer and the security section, and a data receive primitive must be placed between the application layer and the system control section.

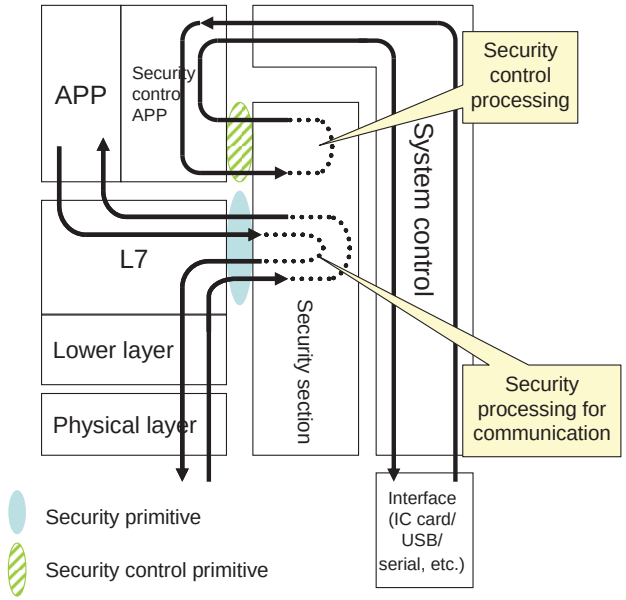


Figure 7-10: Security control application using external interface for security control

c) Security control application using communication for security control

As shown in the illustration below, the security control application uses communication to manage input/output of information required for security control . The following steps are executed.

① After executing security processing for communication between the L7 layer and the security section, the security control data are input to the application layer as application data.

② The application layer receives the data and allocates them to the respective targets (within security control application, within general application).

③ The security control data are analyzed and evaluated by the security control application.

④ The security control data are passed on by the security control application to the security section as required. (Primitive: SecurityCont.Request)

⑤ The security section performs control processing according to the input security control data.

⑥ The security section returns the processing results to the security control application. (Primitive: SecurityCont.Response)

⑦ The security control application the passes processing result data etc. to the L7 layer as required.

In this case, a security control primitive must be placed between the application layer and the security section.

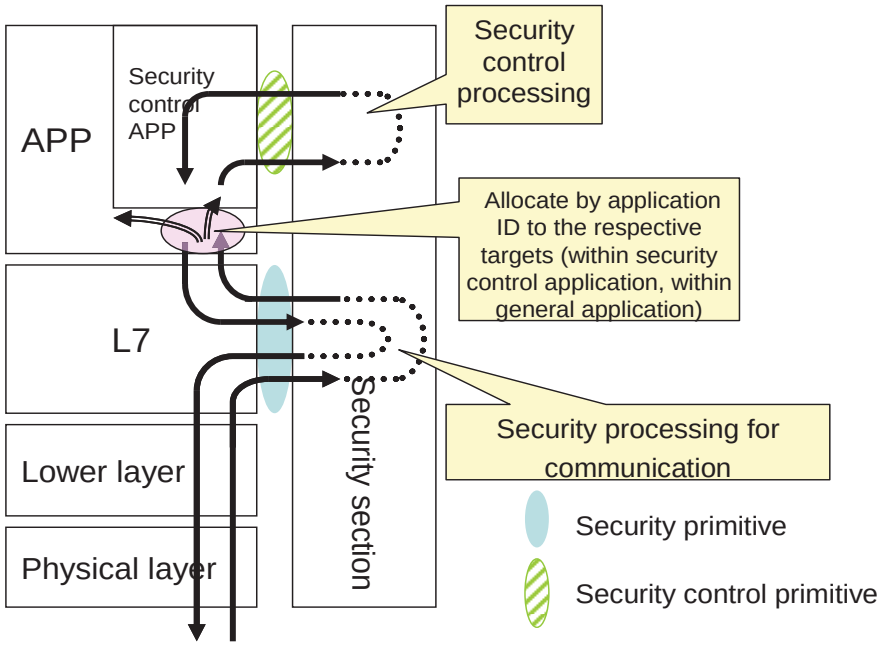


Figure 7-11: Security control application using communication for security control

End of document