ENGLISH TRANSLATION

700 MHz BAND
INTELLIGENT TRANSPORT SYSTEMS

Extended Functions Guideline

ITS FORUM RC-010 Ver. 1.0

Established on March 15, 2012

ITS Info-communications Forum

of Japan

ITS Info-communications Forum

General Notes to the English Translation of ITS Info-communications Forum Guidelines

1. Notes on Copyright

2. Notes on English Translation

- ITS Info-communications Forum Guidelines are usually written in Japanese. This document is a translation into English of the original document for the purpose of convenience of users. If there are any discrepancies in the content, expressions, etc. between the original document and this translated document, the original document shall prevail.

- ITS Info-communications Forum Guidelines, in the original language, are made publicly available through web posting. The original document of this translation may have been further revised and therefore users are encouraged to check the latest version at an appropriate page under the following URL: http://www.itsforum.gr.jp/Public/Eguideline/index.html.

700 MHz BAND
INTELLIGENT TRANSPORT SYSTEMS

Extended Functions Guideline

ITS FORUM RC-010 Ver. 1.0

Established on March 15, 2012

ITS Info-communications Forum

of Japan

Revision History

Ver.	Date	Chapter / Section	Reason	Revised Content
1.0	March 15, 2012	Establishment	Newly established	

[Blank]

Introduction

This guideline defines common specifications and interface specifications of the extended functions implementing the fragmentation and reassembling of application data with the purpose of diversifying applications operating in the context of the "700MHz BAND INTELLIGENT TRANSPORT SYSTEMS" (ARIB STD-T109).

It is hoped that organizations and other parties which utilize the respective standards will perform thorough practical verification and validation testing of the extended functions defined in this guideline, with the expectation of further promoting various activities aimed at the practical realization of the system.

[Blank]

700 MHz BAND INTELLIGENT TRANSPORT SYSTEMS
Extended Functions Guideline

Contents

[Blank]

Chapter 1 General Descriptions

1.1 Outline

The 700 MHz BAND INTELLIGENT TRANSPORT SYSTEMS Extended Functions Guideline (hereinafter referred to as "this Guideline" or "the Guideline") applies to systems implementing the ARIB Standard for 700 MHz BAND INTELLIGENT TRANSPORT SYSTEMS (ARIB STD-T109) (hereinafter referred to as "the Standard"). The Guideline specifies an Extended Layer (hereinafter referred to as "EL”) that extends the protocol functions to include extended functions that enable fragmentation and reassemble processing as well as security management access.

1.2 Scope of application

This Guideline applies to an intelligent transport system (hereinafter referred to as "the system") as defined by the Standard, consisting of a number of base stations and land mobile stations (hereinafter referred to as "mobile station").

The Guideline defines extended functions that reside between the Standard protocol stack and applications, with the purpose of extending the regular protocol functions of the system.

1.3 Normative references

The following standard needs to be referenced in conjunction with this Guideline. The version to use unless otherwise specified is the latest version.

ARIB STD-T109	700 MHz BAND INTELLIGENT TRANSPORT SYSTEMS

[Blank]

Chapter 2 System Outline

2.1 System configuration

The system consists of base stations and mobile stations as defined in the Standard.

2.2 Functions specified by this Guideline

This Guideline implements the following basic system functions.

(1) Application data fragmentation and reassembling functions

(2) Security management access function

2.3 Basic protocol rules

2.3.1 Protocol model

As shown in Figure 2.1, the EL exists as an extended protocol in the hierarchical structure of the system, located between the protocol stack and the application and providing extended communication functions, which results in providing a platform where the application does not need to be aware of the protocol stack.

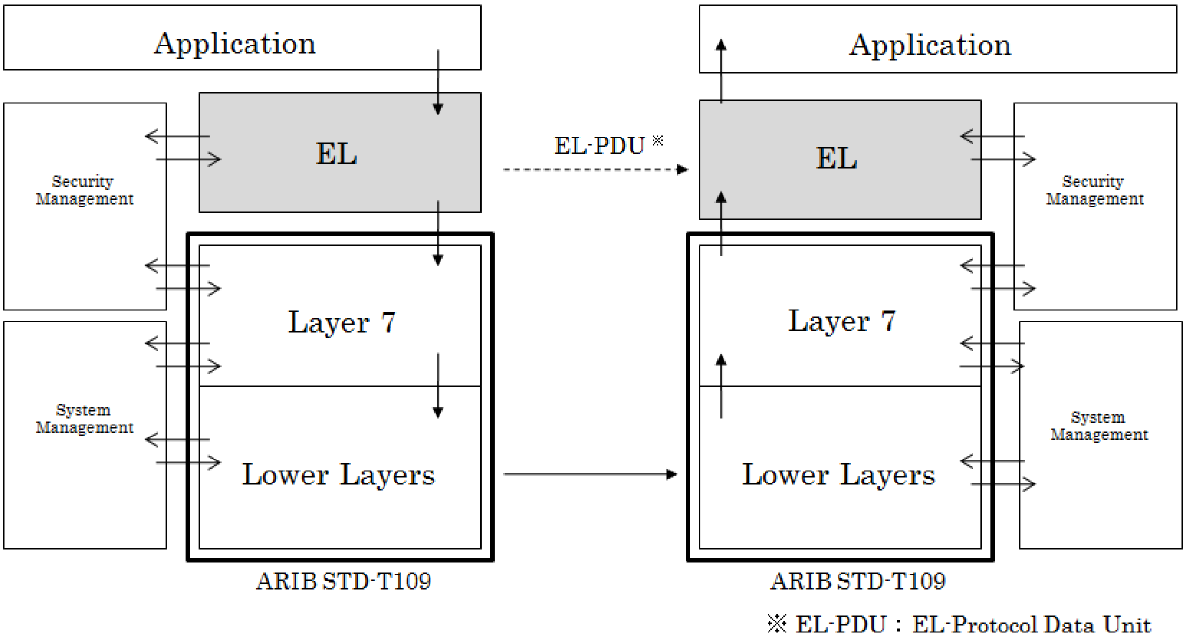


Figure 2.1 Conceptual diagram of EL

2.3.2 Function allocation between EL and Standard Layer 7

As can be seen from Figure 2.1, the Standard Layer 7 has an interface for accessing security management. The EL also has an interface for accessing security management.

When specifying access to data fragmentation and reassembling processing as well as security management, six categories are possible, as listed in Table 2.1. This Guideline, in combination with the Standard, specifies how to implement all of these categories.

Table 2.1 Categories for implementing data fragmentation/reassembling processing and security management

Category	Data fragmentation/ reassembling required	Security management access required	Function distribution between EL and Layer 7
1	Yes	Yes	Data fragmentation/reassembling: EL Security management access: EL
2			Data fragmentation/reassembling: EL Security management access: Layer 7
3	Yes	No	Data fragmentation/reassembling: EL Security management access: Not required
4	No	Yes	Data fragmentation/reassembling: Not required Security management access: EL
5			Data fragmentation/reassembling: Not required Security management access: Layer 7
6	No	No	Data fragmentation/reassembling: Not required Security management access: Not required

2.4 Security method

Not specified in this Guideline.

Chapter 3 Communication Control Method

3.1 Outline

This chapter defines the communication control method of the EL. The interface is defined according to the protocol stack shown in Figure 2.1 of Chapter 2.

The EL provides a data transfer service for the application via the service interface.

The EL uses the service interface provided by the Standard Layer 7 for transmission in protocol data units (EL-PDU: EL Protocol Data Unit) between ELs according to its own specified communication protocol.

3.2 EL standard

3.2.1 Outline

This section defines the EL architecture and service items.

The purpose of the EL is to extend the communication functions of the Standard. For this purpose, it implements the following functions to provide a data transfer service to the application.

- Application data fragmentation and reassembling functions
- Security management access function

3.2.1.1 Composition

The basic structure of the EL and its service access points are shown in Figure 3.1.

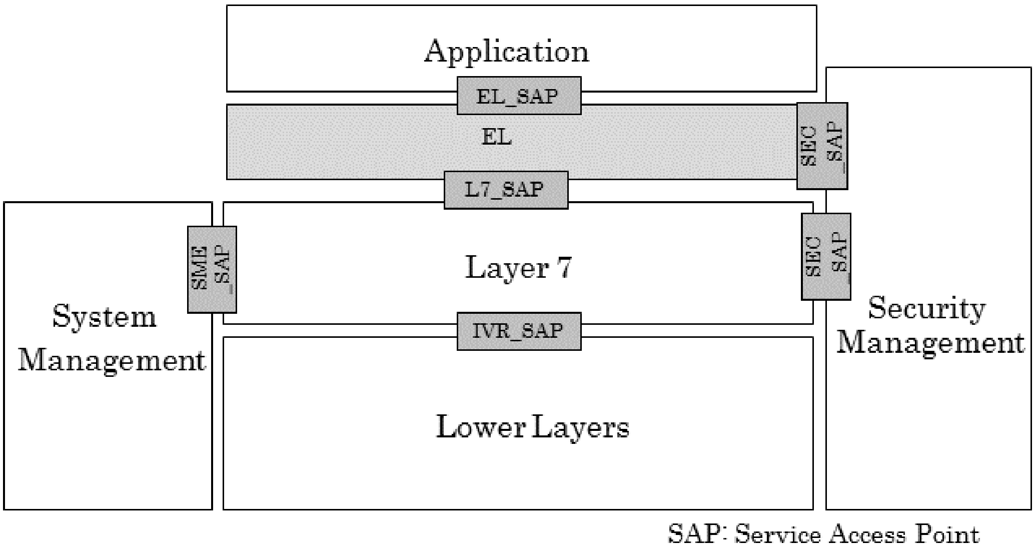


Figure 3.1 Basic structure and service access points of EL

The EL provides a data transfer service to the application via the Extended Layer Service Access Point (EL_SAP). In order to realize the data transfer service, information is communicated as required via the security service access point (SEC_SAP), and then a data transfer request is issued to the next lower layer via the Layer 7 Service Access Point (L7_SAP).

All of these operations are provided to the service user through service primitives.

3.2.1.2 Definition

In this chapter, the user of services provided via the communication protocol stack is defined as the application.

The process of converting local format data to the common transfer syntax used in the communication system, which then is transferred and can be decoded into the local format from transfer syntax format by the service provider at the other end is defined as "encoding". The abstract syntax notation standard ASN.1 [ISO 8824] is used (see Appendix 2).

3.2.2 EL interface service specifications

3.2.2.1 EL data service Interface

3.2.2.1.1 Outline

Data communication between the EL and the application is performed via primitives provided by the EL.

3.2.2.1.2 Outline of mutual relationship of primitives

The following two types of primitives are specified in this section.

- Primitives between application and EL
- Primitives between EL and security management

Figure 3.2 shows the type and the relationship between these primitives.

a) Request

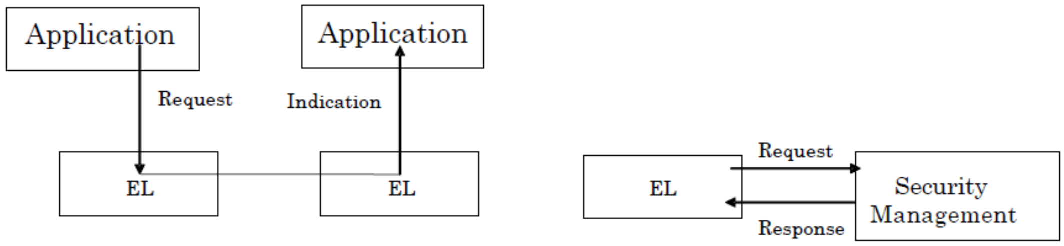
The request primitive is passed from the application to EL, or EL to the security management entity to request a service.

b) Indication

The indication primitive is passed from EL to the application to indicate a service came from another station.

c) Response

The response primitive is passed from the security management entity to EL to send a response with processing results.



(1) Primitives between application and EL

(2) Primitives between EL and Security Management

Figure 3.2 Relationship between primitives and entities

3.2.2.1.3 Service specifications

(1) EL-MobileStationBroadcastData primitive

a) Function

The EL-MobileStationBroadcastData primitive is used for broadcasting by a mobile station application to other applications and for receiving a broadcast from other applications.

b) Format

The format shall be as follows.

EL-MobileStationBroadcastData.request (ControlInformation, EL_SecurityClassification, SecurityInformation, ApplicationAssociatedInformation, EL_ApplicationDataLength, ApplicationData, LinkAddress)

EL-MobileStationBroadcastData.indication (EL_SecurityClassification, SecurityInformation, ApplicationAssociatedInformation, EL_ApplicationDataLength, ApplicationData, LinkAddress, DataAssociatedInformation)

(2) EL-BaseStationBroadcastData primitive

a) Function

The EL-BaseStationBroadcastData primitive is used for broadcasting by a base station application to other applications and for receiving a broadcast from other applications.

b) Format

The format shall be as follows.

EL-BaseStationBroadcastData.request (ControlInformation, EL_SecurityClassification, SecurityInformation, ApplicationAssociatedInformation, EL_ApplicationDataLength, ApplicationData, LinkAddress, DataAssociatedInformation)

EL-BaseStationBroadcastData.indication (EL_SecurityClassification, SecurityInformation, ApplicationAssociatedInformation, EL_ApplicationDataLength, ApplicationData, LinkAddress, DataAssociatedInformation)

(3) EL-Security primitive

a) Function

The EL-Security primitive is used by the EL to transfer application data for which it has received a broadcast request from the application to security management for signing, encryption, or other security processing steps, and then to receive the secure application data. The EL-Security primitive is not called by the application directly but via the EL-MobileStationBroadcastData.request or EL-BaseStationBroadcastData.request.

b) Format

The format shall be as follows.

EL-Security.request (SecurityInformation, ApplicationAssociatedInformation, EL_ApplicationDataLength, ApplicationData)

EL-Security.response (EL_ApplicationDataLength, SecureApplicationData)

(4) EL-Unsecurity primitive

a) Function

The EL-Unsecurity primitive is used by the EL to transfer received secure application data from another station to security management for signature verification, decryption, or other security processing steps, and then to receive the application data. The EL-Unsecurity primitive is not called by the application directly but via the EL-MobileStationBroadcastData.indication or EL-BaseStationBroadcastData.indication.

b) Format

The format shall be as follows.

EL-Unsecurity.request (ApplicationAssociatedInformation, EL_ApplicationDataLength, SecureApplicationData)

EL-Unsecurity.response (SecurityInformation, EL_ApplicationDataLength, ApplicationData)

3.2.2.1.4 Parameters

The parameters for the primitives described in 3.2.2.1.3 are as follows. Unless otherwise specified, the first bit of each data element value in the EL is MSB and the endianness is big-endian.

(1) ControlInformation

See the relevant items in the Standard, section 4.5.2.1.4 Parameters.

(2) EL_SecurityClassification

EL_SecurityClassification shows the security classification information, which is passed from the application to EL. The format of EL_SecurityClassification is shown in Figure 3.3.

Bit	
1	0
EL_SecurityClassification	

b1	b0	Meaning
0	0	No security management access
0	1	Security management access via Layer 7
1	0	Security management access via EL
1	1	Reserved

Figure 3.3 The format of SecurityClassification

(3) SecurityInformation

See the relevant items in the Standard, section 4.5.2.1.4 Parameters.

(4) ApplicationAssociatedInformation

See the relevant items in the Standard, section 4.5.2.1.4 Parameters.

(5) EL_ApplicationDataLength

EL_ApplicationDataLength shows the length of the application data.

EL_ApplicationDataLength is exchanged between the application and EL, or between EL and the security management entity.

The format of ApplicationDataLength is shown in Figure 3.4.

Octet	Bit 7 6 5 4 3 2 1 0
1	EL_ ApplicationDataLength
2	EL_ ApplicationDataLength

Classification	Value	Meaning
EL_ ApplicationDataLength	0-10000 10001-65535	Number of data octets Reserved

Figure 3.4 The format of EL_ApplicationDataLength

(6) ApplicationData

See the relevant items in the Standard, section 4.5.2.1.4 Parameters.

(7) SecureApplicationData

See the relevant items in the Standard, section 4.5.2.1.4 Parameters.

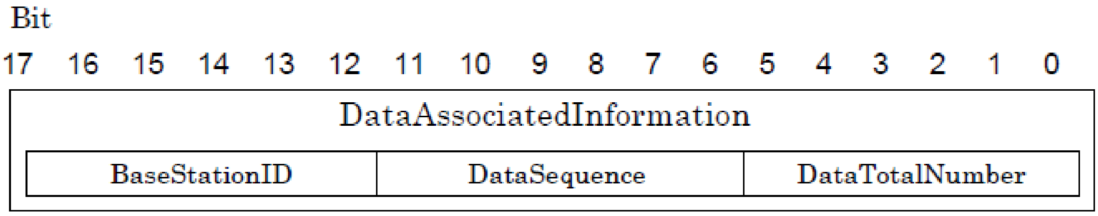
(8) LinkAddress

See the relevant items in the Standard, section 4.5.2.1.4 Parameters.

(9) DataAssociatedInformation

DataAssociatedInformation shows application data associated information. The information is passed between the application and the EL.

The format of DataAssociatedInformation is shown in Figure 3.5.



Classification	Value	Meaning
BaseStationID	1-63	Base station ID Information
DataSequence	1-63	Data sequence information
DataTotalNumber	1-63	Data total number information

Figure 3.5 The format of DataAssociatedInformation

3.2.2.1.5 Sequences

A total of three communication sequence types are used, depending on whether security management is accessed or not, and if it is accessed, whether from the EL or from Layer 7.

The communication sequence that applies when there is no security management access is shown in Figure 3.6. The value of EL_SecurityClassification in this case is 00.

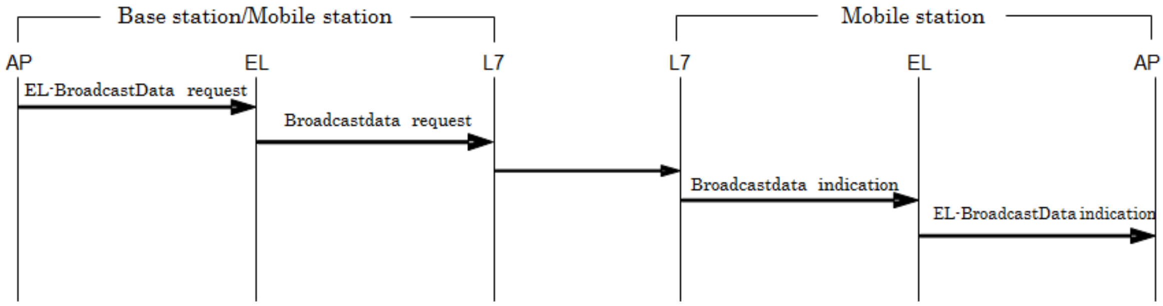


Figure 3.6 Communication sequence without security management access

The communication sequence that applies when there is security management access from the EL is shown in Figure 3.7. The value of EL_SecurityClassification in this case is 10.

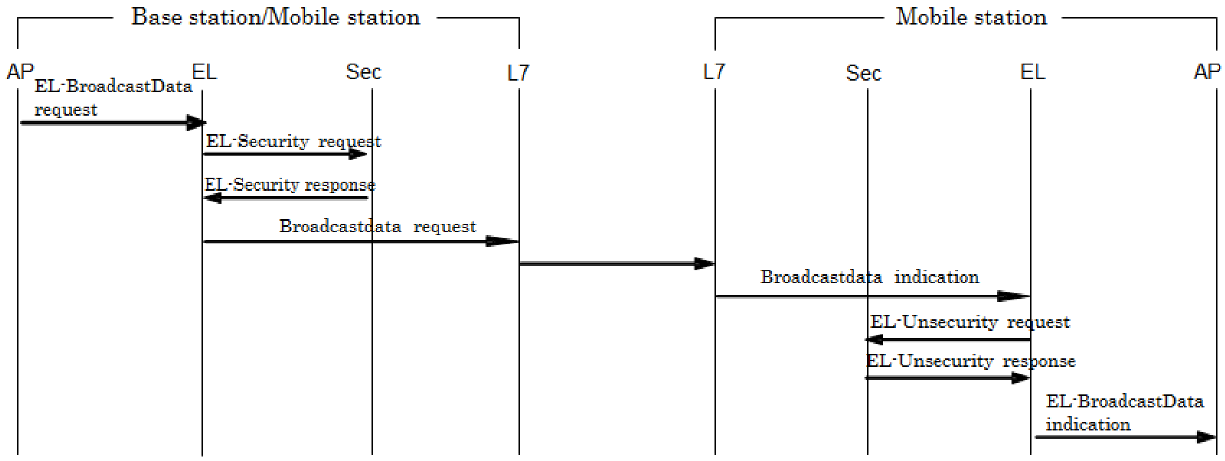


Figure 3.7 Communication sequence with security management access from EL

The communication sequence that applies when there is security management access from Layer 7 is shown in Figure 3.8. The value of EL_SecurityClassification in this case is 01.

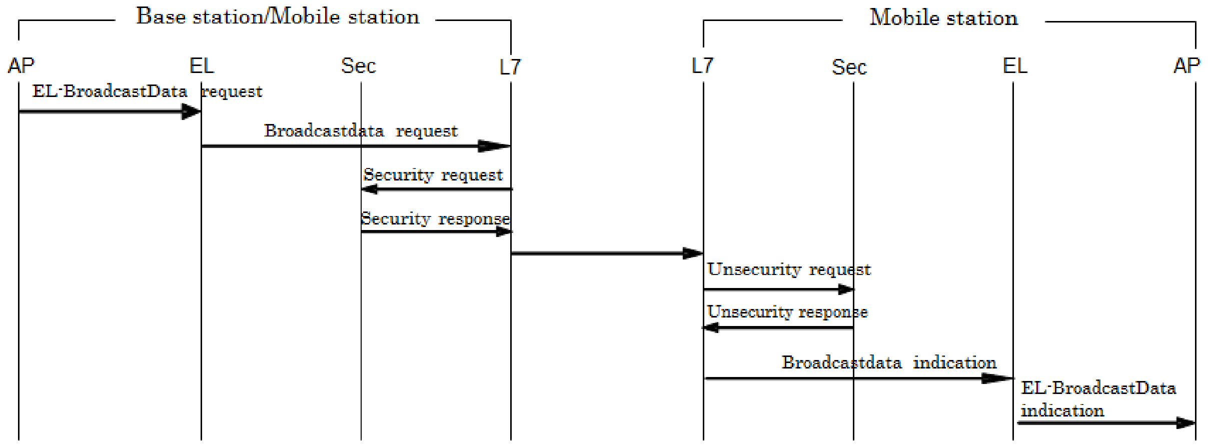


Figure 3.8 Communication sequence with security management access from Layer 7

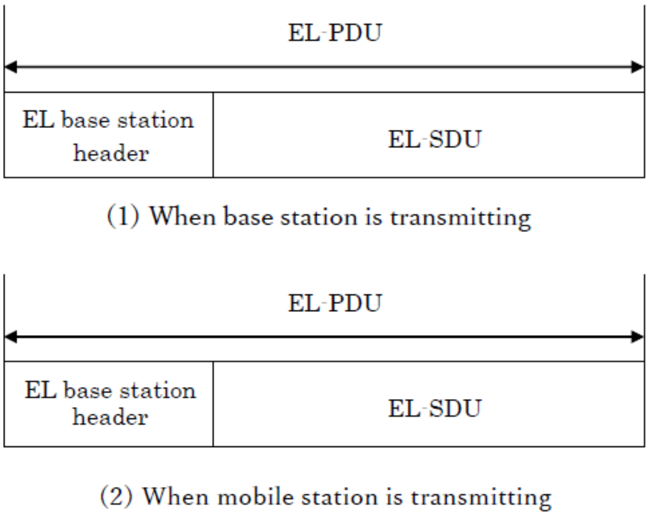
3.2.3 EL communication control

3.2.3.1 Format of EL protocol data unit

For each frame that is sent, the EL receives the EL service data unit (EL-SDU: EL Service Data Unit) from the application and generates the EL protocol data unit (EL-PDU).

As shown in Figure 3.9, when the EL-PDU is sent from the base station, it consists of the EL base station header and the EL-SDU. When the EL-PDU is sent from the mobile station it consists of the EL mobile station header and the EL-SDU.

Unless otherwise specified, the first bit in the EL is MSB and the endianness is big-endian.



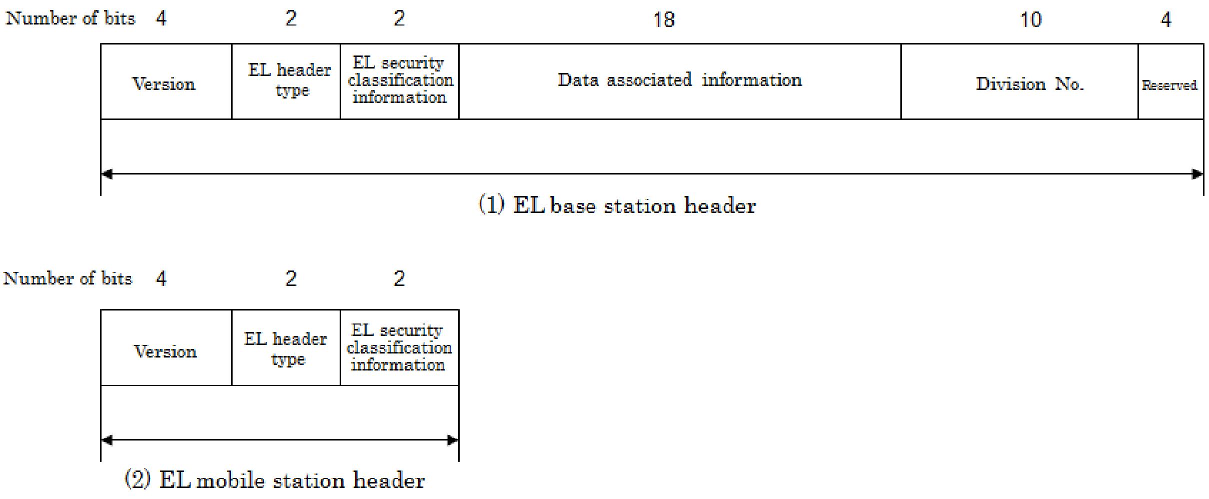
(1) When base station is transmitting

(2) When mobile station is transmitting

Figure 3.9 EL PDU format

3.2.3.2 EL PDU elements

The EL base station header comprises 5 octets and the EL mobile station header comprises 1 octet. The format is shown in Figure 3.10.


Number of bits
4
2
2
18
10
4
Version
EL header type
EL security classification information
Data associated information
Division No.
Reserved
Number of bits
4
2
2
Version
EL header type
EL security classification information

(1) EL base station header

(2) EL mobile station header

Figure 3.10 Format of EL base station header and EL mobile station header

(1) Version

The version value is a field that contains protocol version information for the EL, using the format shown in Figure 3.11.

Bit

3	2	1	0
Version			

Value	Meaning
0	Default
1-15	Reserved

Figure 3.11 Version format

(2) EL header type

The EL header type is a field that contains information for distinguishing the EL base station header from the EL mobile station header, using the format shown in Figure 3.12.

Bit

1	0
EL header type	

b1	b0	Meaning
0	0	Reserved
0	1	EL mobile station header
1	0	EL base station header
1	1	Reserved

Figure 3.12 EL header type format

(3) EL security classification information

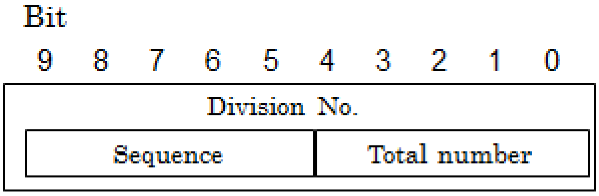
Details are the same as given for EL_SecurityClassification in 3.2.2.1.4, part (2).

(4) Data associated information

Details are the same as given for DataAssociatedInformation in 3.2.2.1.4, part (9).

(5) Fragmentation No.

Fragmentation No. is a field that contains fragmentation information for each application data, using the format shown in Figure 3.13.



Classification	Value	Meaning
Sequence	0-31	Sequence number of fragmented data
Total number	0-31	Total number of fragmented data

Figure 3.13 Fragmentation No. format

(6) Reserved

The value of the reserved field shall be set to 0.

3.2.3.3 EL elements of procedure

(1) Data Fragmentation Size (DDS)

When the EL at the base station performs fragmentation of large application data, this parameter indicates the maximum size of the resulting data segments. The unit is octets. This parameter is to be registered beforehand for each base station as one of the management information base (MIB) parameters specified in Appendix 1.

According to the Standard, the maximum input size for application data in Layer 7 is 1500 octets, and the EL base station header that has to be appended later is 5 octets. The maximum possible DDS value therefore is 1495 octets. The standard value is 1000.

(2) Minimum utilization time of roadside-to-vehicle communication period (SES)

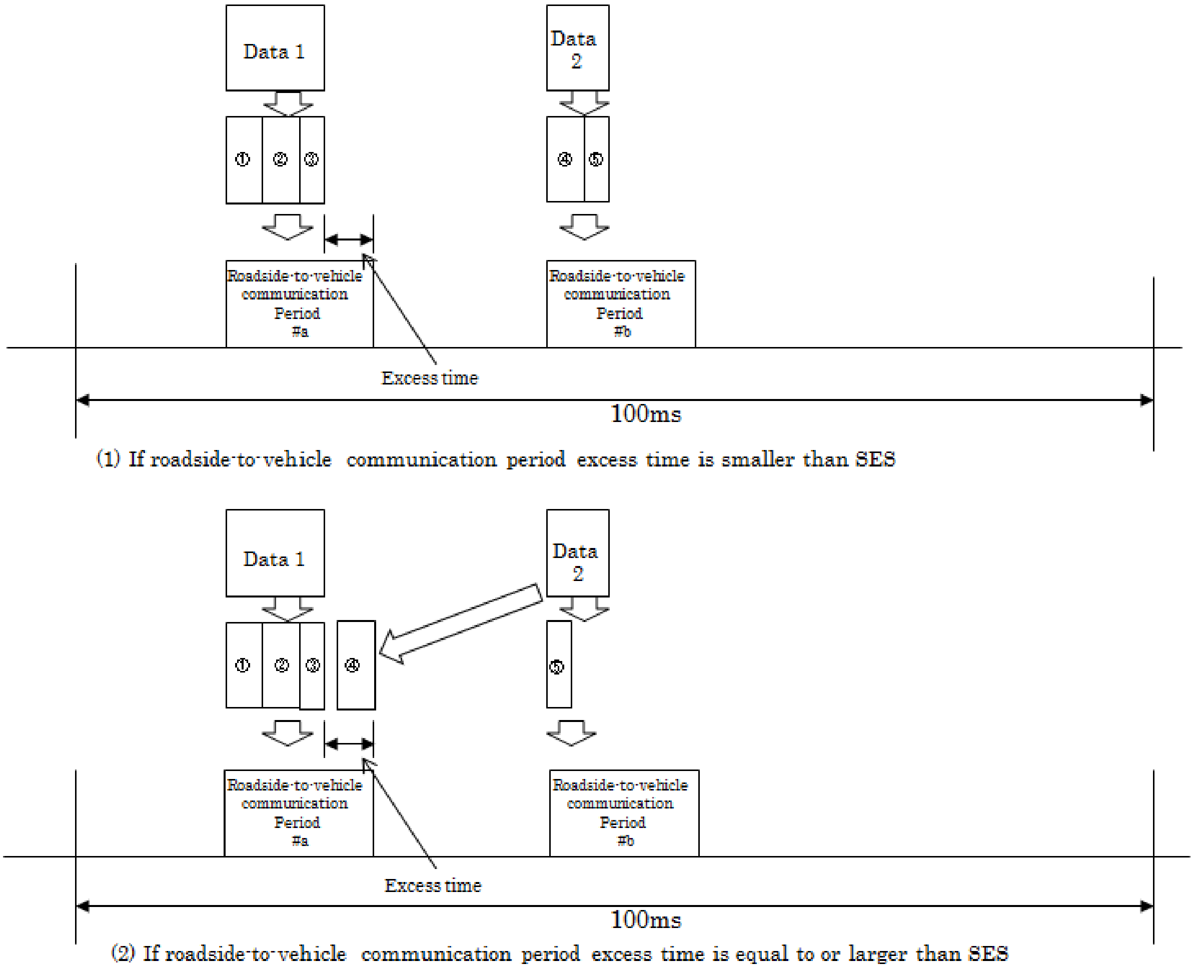
When the EL at the base station performs fragmentation of application data, this parameter serves to evaluate whether an excess of time in the roadside-to-vehicle communication period can be utilized, taking the allocated transmission period (roadside-to-vehicle communication period) for the base station into consideration. The setting is made in μs units, and the SES is set so that it includes one shortest space between transmission frames. This parameter is to be registered beforehand for each base station as one of the management information base (MIB) parameters specified in Appendix 1. Figure 3.14 shows the conceptual diagram of data fragmentation using SES.

The EL calculates the excess time in roadside-to-vehicle communication period, taking parameters such as the overhead of the communication protocol specified by the Standard and modulation method into consideration. The SES parameter is set to a value that is lower than the numerical sum of the time required for transmitting the data of DDS octets (dependent on modulation method) plus the shortest space.

In the example of Figure 3.14, taking data 1 and data 2 as application data and requesting transmission will result in data 1 being fragmented into data ①,②,③, according to the above principle for the DDS parameter. If these are to be allocated to the roadside-to-vehicle communication period #a that can be used by the base station, excess time will be created. In the case of Figure 3.14 (1), if the calculated excess time in the roadside-to-vehicle communication period is smaller than the specified SES, the EL will not use this time period. Rather, data 2 is fragmented into data ④ and ⑤ according to DDS and then allocated to the next roadside-to-vehicle communication period #b.

By contrast, in the case of Figure 3.14 (2), the value of the calculated excess time in the roadside-to-vehicle communication period is larger than the SES value. The EL therefore divides the first part of data 2 into segment data ④, keeping it shorter than the excess time and DDS, and allocates it to roadside-to-vehicle communication period #a. The remaining part is put into data ⑤ according to DDS and allocated to roadside-to-vehicle communication period #b.

The calculation result for the number of roadside-to-vehicle communication periods is given in Reference 1.


Data 1
Data 2
①
②
③
④
⑤
Roadside-to-vehicle communication Period #a
Roadside-to-vehicle communication Period #b
Excess time
100ms

(1) If roadside-to-vehicle communication period excess time is smaller than SES

(2) If roadside-to-vehicle communication period excess time is equal to or larger than SES

Figure 3.14 Conceptual diagram of data fragmentation using SES

3.2.3.4 EL communication control procedure

3.2.3.4.1 Base station

(1) Transmission procedure

a) Generating EL-PDU

According to the EL-BaseStationBroadcastData.request primitive specified in 3.2.2.1.3, the EL shall generate the EL-PDU using the list below, received from the application.

1) ControlInformation

2) EL_SecurityClassification

3) SecurityInformation

4) ApplicationAssociatedInformation

5) EL_ApplicationDataLength

6) ApplicationData

7) LinkAddress

8) DataAssociatedInformation

Depending on the value of 2) EL_SecurityClassification, EL shall carry out one of the following processing routines.

If the EL_SecurityClassification value is 00 or 01, the EL checks the value of 5) EL_ApplicationDataLength.

If the value of 5) EL_ApplicationDataLength is smaller than DDS, 6) ApplicationData shall be taken as EL-SDU, and the EL-PDU shall be generated by prepending the EL base station header specified in 3.2.3.1. to the EL-SDU. In this case, 2) EL_SecurityClassification and 8) DataAssociatedInformation shall be inserted respectively as extended layer security classification information and data associated information in the EL base station header. The Fragmentation No. "Sequence" and "Total Number" items shall be both set to 1.

If the value of 5) EL_ApplicationDataLength is larger than DDS, 6) ApplicationData shall be fragmented according to DDS, and the EL base station header shall be added to each of the resulting segments to generate multiple EL-PDUs. When creating the EL base station header, 2) EL_SecurityClassification and 8) DataAssociatedInformation shall be inserted respectively as extended layer security classification information and data associated information in the EL base station header. The Fragmentation No. information for sequence and total number shall be sequentially added as specified in 3.2.3.2.

If the EL_SecurityClassification value is 10, the EL-Security.request primitive specified in 3.2.2.1.3 shall be called, and 3) SecurityInformation, 4) ApplicationAssociatedInformation, 5) EL_ApplicationDataLength, and 6) ApplicationData shall be sent to security management. The updated new 5) EL_ApplicationDataLength and SecureApplicationData are subsequently received from security management as EL-Security.response primitives, and the value of 5) EL_ApplicationDataLength is checked.

If the value of 5) EL_ApplicationDataLength is smaller than DDS, SecureApplicationData shall be taken as EL-SDU, and the EL-PDU shall be generated by prepending the EL base station header specified in 3.2.3.1. to the EL-SDU. In this case, 2) EL_SecurityClassification and 8) DataAssociatedInformation shall be inserted respectively as extended layer security classification information and data associated information. The Fragmentation No. "Sequence" and "Total Number" items shall be both set to 1.
If the value of 5) EL_ApplicationDataLength is larger than DDS, SecureApplicationData shall be fragmented according to DDS, and the EL base station header shall be added to each of the resulting segments. When creating the EL base station header, 2) EL_SecurityClassification and 8) DataAssociatedInformation shall be inserted respectively as extended layer security classification information and data associated information in the EL base station header. The Fragmentation No. information for sequence and total number shall be sequentially added as specified in 3.2.3.2.

These procedures shall be repeated for each Application Data. Taking the overhead for the communication protocol specified by the Standard into consideration, if there is an excess of time in the Roadside-to-Vehicle communication period, a data fragmentation according to DDS and SES as defined in 3.2.3.3 shall be performed.

Figure 3.15 shows a procedure example for evaluating whether the data fragmentation in the EL has been performed. For case 1 and case 2 in this instance, any new excess time that occurred after the data fragmentation shall be dealt with by repeating this evaluation procedure for the next data.

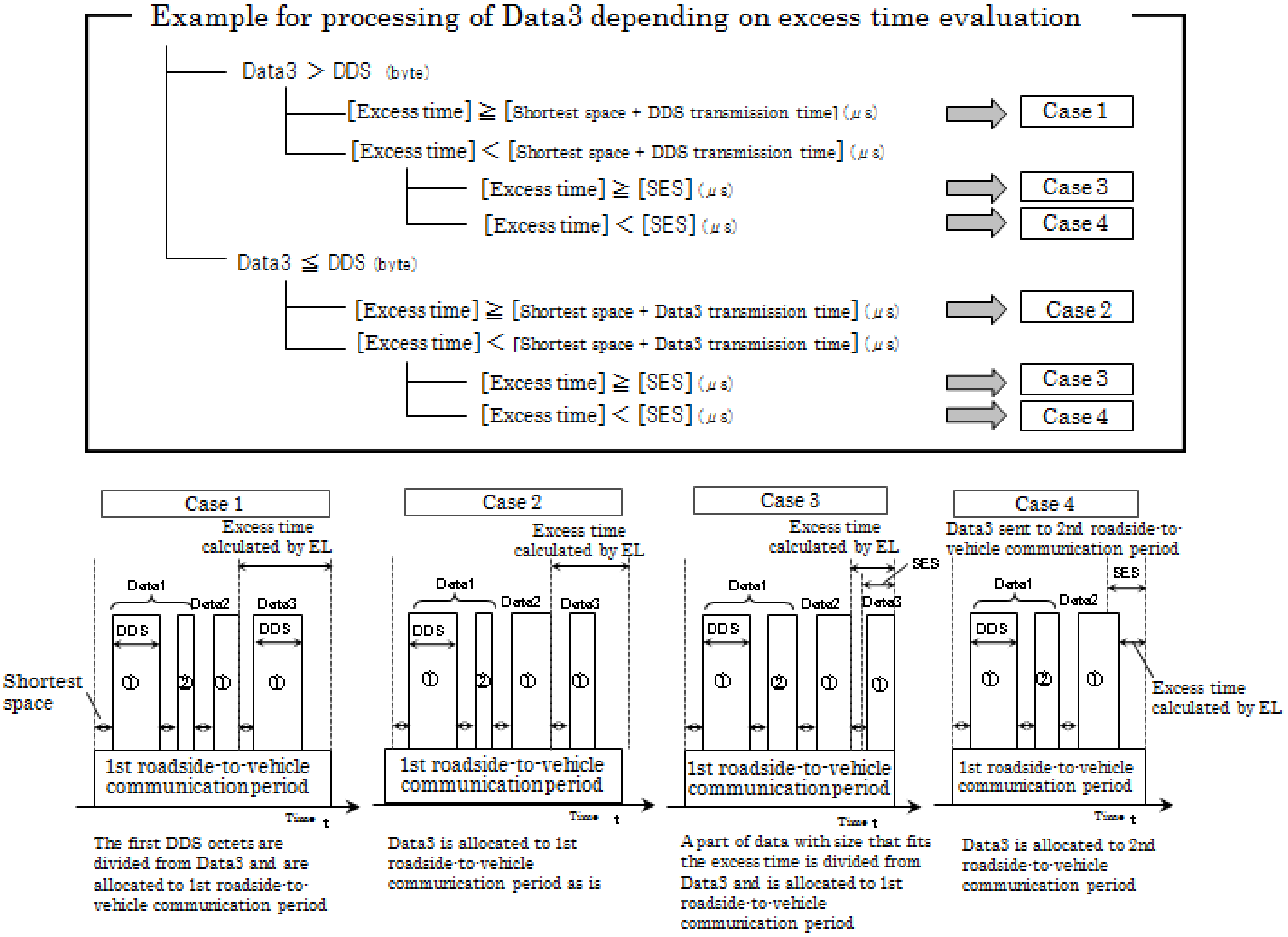

Example for processing of Data3 depending on excess time evaluation
Data3 > DDS (byte)
[Excess time] ≧ [Shortest space + DDS transmission time] (μs)
[Excess time] < [Shortest space + DDS transmission time] (μs)
[Excess time] ≧ [SES] (μs)
[Excess time] < [SES] (μs)
Data3 ≦ DDS (byte)
[Excess time] ≧ [Shortest space + Data3 transmission time] (μs)
[Excess time] < [Shortest space + Data3 transmission time] (μs)
[Excess time] ≧ [SES] (μs)
[Excess time] < [SES] (μs)
Case 1
Case 3
Case 4
Case 2
Case 3
Case 4
Case 1
Excess time calculated by EL
Shortest space
Data1
Data2
Data3
DDS
①
②
1st roadside-to-vehicle communicationperiod
Time t
The first DDS octets are divided from Data3 and are allocated to 1st roadside-to-vehicle communication period
Case 2
Excess time calculated by EL
Data3 is allocated to 1st roadside-to-vehicle communication period as is
Case 3
Excess time calculated by EL
SES
A part of data with size that fits the excess time is divided from Data3 and is allocated to 1st roadside-to-vehicle communication period
Case 4
Data3 sent to 2nd roadside-to-vehicle communication period
SES
Excess time calculated by EL
1st roadside-to-vehicle communication period
Data3 is allocated to 2nd roadside-to-vehicle communication period

Figure 3.15 Data fragmentation evaluation procedure (example)

b) Transmission request to Layer 7

After generating EL-PDU for all transmission data received from the application every 100 ms, a transmission request shall be performed by calling the BaseStationBroadcastData.request primitive of Layer 7. If there are multiple EL-PDUs, a transmission request shall be performed for each EL-PDU. In this case, the EL takes the EL-PDU as ApplicationData and sends it to the BaseStationBroadcastData.request primitive, along with 1) ControlInformation, 3) SecurityInformation, 4) ApplicationAssociatedInformation, 7) LinkAddress received from the application. The EL also sends the following parameters for the BaseStationBroadcastData.request primitive.

Regarding SequenceNumber of the BaseStationBroadcstData.request primitive, the sequence number/total number shall be appended every 100 ms for all data received from the application. A value calculated by adding the EL base station header size to the EL_ApplicationDataLength shall be taken as the ApplicationDataLength of the BaseStationBroadcastData.request primitive. If the EL_SecurityCalssification value is 00 or 10, the SecurityClassification value of the BaseStationBroadcastData.request primitive shall be set to 0. If the EL_SecurityClassification value is 01, the SecurityClassification value of the BaseStationBroadcastData.request primitive shall be set to 1.

(2) Reception procedure

a) Receiving EL-PDU

EL-PDU is received from Layer 7 through the BaseStationBroadcastData indication primitive. At the same time, SecurityClassification, SecurityInformation, ApplicationAssociatedInformation, ApplicationDataLength, and LinkAddress are also received. ApplicationDataLength shall be taken as EL_ApplicationDataLength.

b) Generating EL-SDU

The EL extracts the EL header from the EL-PDU received from Layer 7, and distinguishes between EL base station header and EL mobile station header by checking the EL header type. If the header is an EL base station header, the extended layer security classification information and data associated information shall be taken as EL_SecurityClassification and DataAssociatedInformation and shall be saved along with the Fragmentation No. If the header is an EL mobile station header, the extended layer security classification information shall be saved as EL_SecurityClassification and the "Total Number" item of the Fragmentation No. shall be set to 0.

Next, EL performs one of the following two processing types, depending on the EL_SecurityClassification value.

If the EL_SecurityClassification value is 00 or 01, the EL checks the Fragmentation No. value.

If the "Total Number" item of the Fragmentation No. is 0, the EL-SDU shall be generated by removing the EL mobile station header from the EL-PDU. In this case, EL_ApplicationDataLength for the EL-SDU shall be calculated by subtracting the EL mobile station header size from the value of EL_ApplicationDataLength associated with the EL-PDU.

If the "Total Number" item of the Fragmentation No. is 1, the EL-SDU shall be generated by removing the EL base station header from the EL-PDU. In this case, EL_ApplicationDataLength for the EL-SDU shall be calculated by subtracting the EL base station header size from the value of EL_ApplicationDataLength associated with the EL-PDU.

If the "Total Number" item of the Fragmentation No. is 2 or larger, DataAssociatedInformation is analyzed and the EL-SDU shall be generated by reassembling the results of removing the EL base station header from the EL-PDU for every DataSequence of each BaseStationID, according to the total number and sequence, taking into account the structure of the Fragmentation No. as specified in 3.2.3.2. In this case, EL_ApplicationDataLength of the reassembled EL-SDU shall be calculated by subtracting the EL base station header size from the total value of EL_ApplicationDataLength associated with each EL-PDU. When performing the reassembling operation, the presence of consecutive Fragmentation No. values is to be checked for every DataSequence of each BaseStationID. If a Fragmentation No. is missing, reassembling shall not be performed and all related EL-PDUs shall be discarded. For example, if an EL-PDU sequence comprising 1/5,2/5,3/5, 5/5 is received,4/5 is considered missing, and 1/5,2/5,3/5,5/5 are all discarded.

If the EL_SecurityClassification value is 10, the EL checks the Fragmentation No.

If the "Total Number" item of the Fragmentation No. is 0, the remainder after removing the EL mobile station header from the EL-PDU shall be taken as SecureApplicationData, and the EL mobile station header size shall be subtracted from EL_ApplicationDataLength. Then the EL-Unsecurity.request primitive specified in 3.2.2.1.3 shall be called, and ApplicationAssociatedInformation, EL_ApplicationDataLength, and SecureApplicationData shall be sent to security management. Subsequently, the updated new EL_ApplicationDataLength, SecurityInformation, and ApplicationData are received as the EL-Unsecurity.response primitive from security management. The EL takes these ApplicationData as the EL-SDU.

If the "Total Number" item of the Fragmentation No. is 1, the remainder after removing the EL base station header from the EL-PDU shall be taken as SecureApplicationData, and the EL base station header size shall be subtracted from EL_ApplicationDataLength. Then the EL-Unsecurity.request primitive specified in 3.2.2.1.3 shall be called, and ApplicationAssociatedInformation, EL_ApplicationDataLength, and SecureApplicationData shall be sent to security management. Subsequently, the updated new EL_ApplicationDataLength, SecurityInformation, and ApplicationData are received as the EL-Unsecurity.response primitive from security management. The EL takes these ApplicationData as the EL-SDU.

If the "Total Number" item of the Fragmentation No. is 2 or larger, DataAssociatedInformation is decomposed and SecureApplicationData shall be generated by reassembling the results of removing the EL base station header from the EL-PDU for every DataSequence of each BaseStationID, according to the total number and sequence, taking into account the structure of the Fragmentation No. as specified in 3.2.3.2. In this case, EL_ApplicationDataLength of the reassembled SecureApplicationData shall be calculated by subtracting the EL base station header size from the total value of EL_ApplicationDataLength associated with each EL-PDU. When the reassembling operation is completed, the EL-Unsecurity.request primitive specified in 3.2.2.1.3 shall be called, and ApplicationAssociatedInformation, EL_ApplicationDataLength, and SecureApplicationData shall be sent to security management. Subsequently, the updated new EL_ApplicationDataLength, SecurityInformation, and ApplicationData are received as the EL-Unsecurity.response primitive from security management. The EL takes these ApplicationData as the EL-SDU.

c) Reception notification to application

The EL shall notify applications of reception by using the EL-BaseStationBroadcastData.indication primitive.

If the received EL-PDU has an EL mobile station header, the EL-SDU shall be taken as ApplicationData and shall be sent to the application, along with

EL_SecurityClassification, SecurityInformation, ApplicationAssociatedInformation, EL_ApplicationDataLength, LinkAddress, and DataAssociatedInformation.

If the received EL-PDU has an EL base station header, the EL-SDU shall be taken as ApplicationData for each DataSequence of the BaseStationID, and shall be sent to the application, along with EL_SecurityClassification, SecurityInformation, ApplicationAssociatedInformation, EL_ApplicationDataLength, LinkAddress, and DataAssociatedInformation.

3.2.3.4.2 Mobile station

(1) Transmission procedure

a) Generating EL-PDU

According to the EL-MobileStationBroadcastData.request primitive specified in 3.2.2.1.3, the EL shall generate the EL-PDU using the list below, received from the application.

1) ControlInformation
2) EL_SecurityClassification
3) SecurityInformation
4) ApplicationAssociatedInformation
5) EL_ApplicationDataLength
6) ApplicationData
7) LinkAddress

Depending on the value of 2) EL_SecurityClassification, EL shall carry out one of the following processing routines.

If the EL_SecurityClassification value is 00 or 01, 6) ApplicationData shall be taken as EL-SDU, and the EL-PDU shall be generated by prepending the EL-SDU with the EL mobile station header specified in 3.2.3.1. In this case, 2) EL_SecurityClassification shall be inserted as extended layer security classification information in the EL mobile station header.

If the EL_SecurityClassification value is 10, the EL-Security.request primitive specified in 3.2.2.1.3 shall be called, and 3) SecurityInformation, 4)

ApplicationAssociatedInformation, 5) EL_ApplicationDataLength, and 6) ApplicationData shall be sent to security management. The updated new 5) EL_ApplicationDataLength and SecureApplicationData are subsequently received from security management as EL-Security.response primitives, SecureApplicationData shall be taken as EL-SDU, and the EL-PDU shall be generated by prepending the EL-SDU with the EL mobile station header specified in 3.2.3.1. In this case, 2) EL_SecurityClassification shall be inserted as extended layer security classification information in the EL mobile station header.

b) Transmission request to Layer 7

After generating the EL-PDU, a transmission request shall be performed by calling the BaseStationBroadcastData.request primitive of Layer 7. In this case, the EL takes EL-PDU as ApplicationData and sends it to the MobileStationBroadcastData.request primitive, along with 1) ControlInformation, 3) SecurityInformation, 4) ApplicationAssociatedInformation, and 7) LinkAddress received from the application. The EL also sends the following parameters for the MobileStationBroadcastData.request primitive.

The ApplicationDataLength parameter for the MobileStationBroadcastData.request primitive shall be generated by adding the EL mobile station header size to EL_ApplicationDataLength. If the EL_SecurityClassification value is 00 or 10, the SecurityClassification value of the MobileStationBroadcastData.request primitive shall be set to 0. If the EL_SecurityClassification value is 01, the SecurityClassification value of the MobileStationBroadcastData.request primitive shall be set to 1.

(2) Reception procedure

a) Receiving EL-PDU

EL-PDU is received from Layer 7 through the MobileStationBroadcastData indication primitive. At the same time, SecurityClassification, SecurityInformation, ApplicationAssociatedInformation, ApplicationDataLength, and LinkAddress are also received. ApplicationDataLength shall be taken as EL_ApplicationDataLength.

b) Generating EL-SDU

The EL extracts the EL header from the EL-PDU received from Layer 7, and distinguishes between EL base station header and EL mobile station header by checking the EL header type. If the header is an EL base station header, the extended layer security classification information and data associated information shall be taken as EL_SecurityClassification and DataAssociatedInformation and shall be saved along with the Fragmentation No. If the header is an EL mobile station header, the extended layer security classification information shall be saved as EL_SecurityClassification and the "Total Number" item of the Fragmentation No. shall be set to 0.

Next, EL performs one of the following two processing types, depending on the EL_SecurityClassification value.

If the EL_SecurityClassification value is 00 or 01, the EL checks the Fragmentation No. value.

If the "Total Number" item of the Fragmentation No. is 0, the EL-SDU shall be generated by removing the EL mobile station header from the EL-PDU. In this case, EL_ApplicationDataLength of the EL-PSU shall be calculated by subtracting the EL mobile station header size from the value of EL_ApplicationDataLength associated with the EL-PDU.

If the "Total Number" item of the Fragmentation No. is 1, the EL-SDU shall be generated by removing the EL base station header from the EL-PDU. In this case, EL_ApplicationDataLength of the EL-PSU shall be calculated by subtracting the EL base station header size from the value of EL_ApplicationDataLength associated with the EL-PDU.

If the "Total Number" item of the Fragmentation No. is 2 or larger, DataAssociatedInformation is decomposed and the EL-SDU shall be generated by reassembling the results of removing the EL base station header from the EL-PDU for every DataSequence of each BaseStationID, according to the total number and sequence, taking into account the structure of the Fragmentation No. as specified in 3.2.3.2. In this case, EL_ApplicationDataLength of the reassembled EL-SDU shall be calculated by subtracting the EL base station header size from the total value of EL_ApplicationDataLength associated with each EL-PDU. When performing the reassembling operation, the presence of consecutive Fragmentation

No. values is to be checked for every DataSequence of each BaseStationID. If a Fragmentation No. is missing, reassembling shall not be performed and all related EL-PDUs shall be discarded. For example, if an EL-PDU sequence comprising 1/5,2/5,3/5, 5/5 is received,4/5 is considered missing, and 1/5,2/5,3/5,5/5 are all discarded.

If the EL_SecurityClassification value is 10, the EL checks the Fragmentation No.

If the "Total Number" item of the Fragmentation No. is 0, the remainder after removing the EL mobile station header from the EL-PDU shall be taken as SecureApplicationData, and the EL mobile station header size shall be subtracted from EL_ApplicationDataLength. Then the EL-Unsecurity.request primitive specified in 3.2.2.1.3 shall be called, and ApplicationAssociatedInformation, EL_ApplicationDataLength, and SecureApplicationData shall be sent to security management. Subsequently, the updated new EL_ApplicationDataLength, SecurityInformation, and ApplicationData are received as the EL-Unsecurity.response primitive from security management. The EL takes these ApplicationData as the EL-SDU.

If the "Total Number" item of the Fragmentation No. is 1, the remainder after removing the EL base station header from the EL-PDU shall be taken as SecureApplicationData, and the EL base station header size shall be subtracted from EL_ApplicationDataLength. Then the EL-Unsecurity.request primitive specified in 3.2.2.1.3 shall be called, and ApplicationAssociatedInformation, EL_ApplicationDataLength, and SecureApplicationData shall be sent to security management. Subsequently, the updated new EL_ApplicationDataLength, SecurityInformation, and ApplicationData are received as the EL-Unsecurity.response primitive from security management. The EL takes these ApplicationData as the EL-SDU.

If the "Total Number" item of the Fragmentation No. is 2 or larger, DataAssociatedInformation is decomposed and SecureApplicationData shall be generated by reassembling the results of removing the EL header from the EL-PDU for every DataSequence of each BaseStationID, according to the total number and sequence, taking into account the structure of the Fragmentation No. as specified in 3.2.3.2. In this case, EL_ApplicationDataLength of the reassembled

SecureApplicationData shall be calculated by subtracting the EL base station header size from the total value of EL_ApplicationDataLength associated with each EL-PDU. When the reassembling operation is completed, the EL-Unsecurity.request primitive specified in 3.2.2.1.3 shall be called, and ApplicationAssociatedInformation, EL_ApplicationDataLength, and SecureApplicationData shall be sent to security management. Subsequently, the updated new EL_ApplicationDataLength, SecurityInformation, and ApplicationData are received as the EL-Unsecurity.response primitive from security management. The EL takes these ApplicationData as the EL-SDU.

c) Reception notification to application

The EL shall notify the application of reception by using the EL-MobileStationBroadcastData.indication primitive.

If the received EL-PDU has an EL mobile station header, the EL-SDU shall be taken as ApplicationData and shall be sent to the application, along with EL_SecurityClassification, SecurityInformation, ApplicationAssociatedInformation, EL_ApplicationDataLength, LinkAddress, and DataAssociatedInformation.

If the received EL-PDU has an EL base station header, the EL-SDU shall be taken as ApplicationData for each DataSequence of the BaseStationID, and shall be sent to the application, along with EL_SecurityClassification, SecurityInformation, ApplicationAssociatedInformation, EL_ApplicationDataLength, LinkAddress, and DataAssociatedInformation.

Appendix 1 Management Information Base (MIB)

Parameters	Meaning	Type	Length	Value	Remarks
DDS	Data Fragmentation Size (DDS)	BIT STRING	16 bit	1 to 1495	Unit: octet
SES	Minimum utilization time of roadside-to-vehicle communication period (SES)	BIT STRING	16 bit	32 to 2000	Unit: μs

[Blank]

Appendix 2　Application data structure definitions

1　Mobile station broadcast application data

```
EL-MobileStationBroadcastData DEFINITIONS ::=
BEGIN

ControlInformation ::= SEQUENCE{
        DataRate        DataRateParameter
        reserve         INTEGER(0..15)          -- Reserved for future use
}
-- Radio parameter (modulation) control information

DataRateParameter ::= INTEGER {
        BPSK1/2         (1)
        BPSK3/4         (2)
        QPSK1/2         (0),
        QPSK3/4         (3),
        16QAM1/2        (4),
        16QAM3/4        (5),

        -- Values 6 to 15 of DataRateParameter are reserved
}(0..15)

EL_SecurityClassification ::= INTEGER {
        (0)     -- No security management access
        (1)     -- Security management access via Layer 7
        (2)     -- Security management access via EL
        (3)     Reserved
}(0..3)

SecurityInformation ::= OCTET STRING(SIZE(20))
-- Security information
```

```
ApplicationAssociatedInformation ::= BIT STRING(SIZE(8))
-- Application associated information

EL_ApplicationDataLength ::= INTEGER(0..10000)
-- Application data length

ApplicationData ::= OCTET STRING(SIZE(0..10000))
-- Application data

LinkAddress ::= OCTET STRING(SIZE(6))
-- Destination link address

END
```

2 Base station broadcast application data

```
EL-BaseStationBroadcastData DEFINITIONS ::=
BEGIN

ControlInformation ::= SEQUENCE{
        DataRate            DataRateParameter
        reserve             INTEGER(0..15)          -- Reserved for future use
}
-- Radio parameter (modulation) control information

DataRateParameter ::= INTEGER {
        BPSK1/2             (1)
        BPSK3/4             (2)
        QPSK1/2             (0),
        QPSK3/4             (3),
        16QAM1/2            (4),
        16QAM3/4            (5),
  -- Values 6 to 15 of DataRateParameter are reserved
  }(0..15)

  EL_SecurityClassification ::= INTEGER {
        (0)       -- No security management access
        (1)       -- Security management access via Layer 7
        (2)       -- Security management access via EL
        (3)       Reserved
  }(0..3)

  SecurityInformation ::= OCTET STRING(SIZE(20))
  -- Security information

  ApplicationAssociatedInformation ::= BIT STRING(SIZE(8))
  -- Application associated information

  EL_ApplicationDataLength ::= INTEGER(0..10000)
  -- Application data length

  ApplicationData ::= OCTET STRING(SIZE(0..10000))
  -- Application data

  LinkAddress ::= OCTET STRING(SIZE(6))
  -- Destination link address

  DataAssociatedInformation ::= SEQUENCE{
        BaseStationID           INTEGER(1.. 63)                 -- Base station ID
information
        DataSequence            INTEGER(1.. 63)                 -- Data sequence
information
        DataTotalNumber         INTEGER(1.. 63)                 -- Data total number
information
  }
```

END

[Blank]

Reference 1 Calculation results for number of roadside-to-vehicle communication periods

This section explains the results of calculating the number of roadside-to-vehicle communication periods used by the base station.

The length of the application data in the extended layer can be 0 to 10000 octets (see 3.2.2.1.4). Further, the maximum length of one roadside-to-vehicle communication period is 3024 µs (See the Standard, section 4.4.3.1.2). Consequently, if the application data length exceeds the size that can be transmitted in one roadside-to-vehicle communication period, multiple periods must be used. The user of roadside-to-vehicle communications therefore must take the number of roadside-to-vehicle communication periods that can be used by one base station into account when setting the application data length.

An example for calculating the required number of roadside-to-vehicle communication periods when sending one application data from one base station is given below.

1. Calculation parameters

- Length of each header and footer

(See the Standard. For EL base station header length, see this Guideline, section 3.2.3.2.)

Table 1 Header and footer length parameters

Setting unit	Header/footer name	Header/footer length [octets]
Per frame	MAC control field	24
	LLC control field	8
	IR control field	22
	L7 header	2
	EL base station header	5
	FCS field	4

- Roadside-to-vehicle communication period length: 3024 [µs]
- Shortest space: 32 [µs] (See the Standard, section 4.3.4.3.1)
- Modulation method (coding rate): 16QAM (1/2)
- SES: 600 µs (See section 3.2.3.3, part (2))

2. Calculation example for number of roadside-to-vehicle communication periods

The extended layer performs fragmentation of application data, according to DDS (See section 3.2.3.3, part (2)).Using the calculation parameters listed in section 1., this section shows the results of calculating the number of roadside-to-vehicle communication periods required for each application data length, for two cases: (a) DDS = 1300 octets, and (b) DDS = 1000 octets.

The burst length for sending a frame is 952 [μs] when the DDS is 1300 octets, and 752 [μs] when the DDS is 1000 octets.

Table 2 Calculation of required roadside-to-vehicle communication periods depending on application data length

(a) DDS = 1300 [octets]

Application data length [octets]	Possible number of frames	Number of roadside-to-vehicle communication periods
3900	3	1
7800	6	2
10000	8	3

(b) DDS = 1000 [octets]

Application data length [octets]	Possible number of frames	Number of roadside-to-vehicle communication periods
3000	3	1
6000	6	2
9000	9	3
10000	10	4

The calculations in Table 2 are based on the rule stated in 3.2.3.3, part (2), which specifies that if the excess time in the roadside-to-vehicle communication period is smaller than the sum of the shortest space and the DDS transmission time, and smaller than SES, the transmission frame will not be allocated to the excess time but rather to the next roadside-to-vehicle communication period.

If the excess time in the roadside-to-vehicle communication period is smaller than the sum of the shortest space and the DDS transmission time, but larger than SES, a transmission frame with a size that fits the excess time will be generated and allocated to the excess time (see Figure 3).

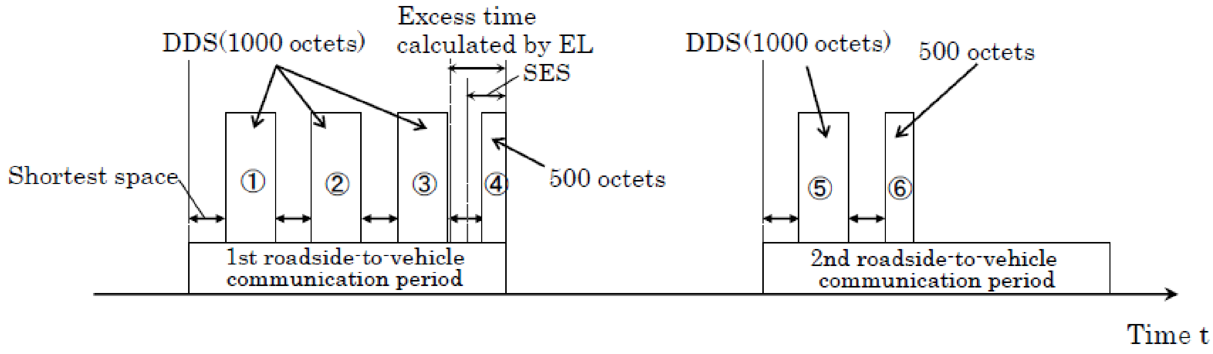


Figure 3 Operation when SES ≦ Excess time in roadside-to-vehicle communication period < sum of shortest space and DDS transmission time