Road Communication Standards :

Protocol Standard (Ver.1.05)

February 2006 National Institute for Land and Infrastructure Management Ministry of Land, Infrastructure and Transport

Contents

1	Purpose									
2	Scope	3								
	2.1 System Models	3								
	2.2 Standard Protocol Selection Criteria	4								
3	References	5								
4	Terms and Abbreviation	9								
	4.1 Terms and Definitions									
	4.2 Abbreviation and Definitions	10								
5	Protocol									
	5.1 Protocol Set	11								
	5.1.1 Lower Layer Protocol Set	11								
	5.1.2 Upper Layer Protocol Set	17								
	5.2 Protocol Set Combination	19								
6	Protocol Detail	21								
	6.1 DATEX-ASN	21								
	6.1.1 DATEX-ASN Protocol Detail	21								
	6.1.2 DATEX-ASN Message Sequence									
	6.1.3 State Transition	44								

Appendix:DATEX-ASN Data Packet Details

1 Purpose

Road Communication Standards : Protocol Standard (hereafter "this standard") is a protocol determined on the basis of various communication requirements to be applied to the ITS system procured by the road agencies in Japan. Its objective is to bring about an improvement in the efficiency of selecting a protocol for the systems procured by various road agencies as well as ensuring interconnectivity with respect to protocols.

As expressed by Figure 1-1 the protocol is closely associated with a data dictionary (DD) and message set (MS) included in the Road Communication Standards. These three kinds of standards will serve to ensure improved efficiency of system design and interconnectivity and to simplify the procurement process of equipment.

However, this standard is not something that will negate, amend or regulate with respect to protocols that are being used in systems already possessed by road operators. Moreover, protocols for use in the operation and management systems are outside the scope of this standard.



Figure 1-1: Relationship of the protocol (PT) with DD and MS

2 Scope

2.1 System Models

This standard applies to the following system models.

No	System Model Names
1	System to offer advance notice of road-related information
2	System to connect with another organization
	- (1) System to offer information related to parking lot
3	System to connect with another organization
	- (2) System to provide public traffic information
4	System to connect with another organization
	- (3) System to provide information about highway buses
5	System to connect with another organization
	- (4) System to provide information about another organization
6	Administrative procedures for specially permitted vehicles
	- (1) System to support EDI for commercial vehicles
7	Administrative procedures for specially permitted vehicles
	- (2) System for administration of specially permitted vehicles
8	System to monitor overloaded vehicles
9	System to support road administration
10	System to grasp the road environmental information
11	System to conduct disaster management
12	Advance highway safety system for cold districts
13	System to detect unforeseen accidents
14	System to offer information related to road
15	System to offer an optimal path information
16	System for traffic control
17	System for traffic management of specific occurrences
18	System for automatic toll collection
19	System to support public transport operation
20	System to support pedestrian

2.2 Standard Protocol Selection Criteria

Standards for communication protocols to be applied in the systems shown in section 2.1 have been selected based on the followings:

- (1) Learning from the recent spectacular proliferation of the Internet and Intranet and their serviceability, an internet protocol (IP) shall be used as layer 3 of the open system interconnection (OSI) basic reference model of ISO.
- (2) The protocols unable to support high speed services, such as half duplex, asynchronous and character synchronous, are excluded from this standard.
- (3) Since IP has been adopted as layer-3 protocol, protocols with high IP affinity are applied for other layers, i.e. layers 1 to 2, and 4 to 7.
- (4) The widespread use of optical fiber in recent years has increased the speed of transmission media and brought about advanced digital multiplexing. Therefore, in this standard, the protocols shall be determined by prioritizing "services which communication functions provide" over "effective use of communication circuits".

3 References

Reference standards for protocols specified in this standard are shown below.

- (1) ATM
 - ITU-T Recommendation I.361 (02/99) B-ISDN ATM layer specification
 - ITU-T Recommendation I.363 (03/93) B-ISDN ATM adaptation layer (AAL) specification
 - ITU-T Recommendation I.413 (03/93) B-ISDN user-network interface
 - ITU-T Recommendation I.432.1 (02/99) B-ISDN user-network interface Physical layer specification: General characteristics
- (2) BER
 - JIS X 5606-1:1998 Information technology ASN.1 encoding rules -Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) (ISO/IEC 8825-1:1995 Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER))
- (3) CER

• the same as (2)

- (4) DER
 - the same as (2)
- (5) DSRC
 - Association of Radio Industries and Businesses(ARIB) STD-T55 --ELECTRONIC TOLL COLLECTION SYSTEM
 - Association of Radio Industries and Businesses(ARIB) STD-T75 --DEDICATED SHORT RANGE COMMUNICATION (DSRC) SYSTEM
- (6) Ethernet
 - 8802-3:1996 (ISO/IEC)[ANSI/IEEE Std 802.3, 1996 Edition] Information technology -- Telecommunications and information exchange between system -- Local and Metropolitan area networks --Specific requirement -- Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.
 - EIA/TIA568B (AT and T-258A) Commercial Building Telecommunications Wiring Standard, 1991

- (7) Fast Ethernet
 - IEEE 802.3u-1995 IEEE Standards for Local and metropolitan area networks: Supplement to Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: Media access control (MAC) Parameters, Physical Layer, Medium Attachment Units, and Repeater for 100 Mb/s Operation, Type 100BaseT (Clauses 21-30)(ANSI)
 - EIA/TIA568B (AT and T-258A) Commercial Building Telecommunications Wiring Standard, 1991
- (8) FDDI
 - ANSI X3.166-1989(R1995) Fiber Distributed Data Interface (FDDI) Physical Layer Medium Dependent (PMD)
 - ANSI X3.148-1988 (R1994) Information Systems Fiber Distributed Data Interface (FDDI) - Token Ring Physical Layer Protocol (PHY)
 - ANSI X3.139-1987 (R1997) Information Systems Fiber Distributed Data Interface (FDDI) Token Ring Media Access Control (MAC)
 - ISO/IEC 9314-3:1990 Information Processing systems Fiber distributed Data Interface (FDDI) Part 3: Physical Layer Medium Department (PMD)
 - ISO 9314-2:1989 Information processing systems Fiber Distributed Data Interface (FDDI) - Part 2: Token Ring Media Access Control (MAC)
 - ISO 9314-1:1989 Information processing systems Fiber Distributed Data Interface (FDDI) - Part 1: Token Ring Physical Layer Protocol (PHY)
- (9) FTP
 - RFC 959 File Transfer Protocol, J. Postel, J.K. Reynolds, Oct-01-1985 (Status: STANDARD)
- (10) Gigabit Ethernet
 - IEEE 802.3ab : Physical coding sublayer(PCS), physical medium attachment(PMA)sublayer and baseband medium, type 1000BASE-T
 - IEEE 802.3z : Media Access Control(MAC) Parameters, Physical Layer, Repeater and Management Parameters for 1000 Mb/s Operation
- (11) G.703a
 - TTC JT-G703-a Leased Line Secondary Rate User-Network Interface Layer 1.
- (12) HTTP
 - RFC 1945 Hypertext Transfer Protocol -- HTTP/1.0. R. Fielding, H.

Frystyk, T. Berners-Lee, May 1996 (Status: INFORMATION)

- RFC 2068 Hypertext Transfer Protocol -- HTTP/1.1. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, T. Berners-Lee, January 1997 (Status: PROPOSED STANDARD)
- (13) H.261
 - ITU-T Recommendation H.261(1993),Video codec for audiovisual services at p x 64kbit/s
- (14) IP
 - RFC 791 Internet Protocol. J. Postel. Sep-01-1981 (Status: STANDARD)
- (15) I.430
 - TTC JT-I430 ISDN Basic User-Network Interface Layer 1.
- (16) I.431
 - TTC JT-I431-a ISDN Primary-Rate User-Network Interface Layer1.
- (17) M-JPEG
 - ISO-IEC 10918-1:1994 Information technology Digital compression and coding of continuous-tone still images: Requirements and gridlines.
 - ITU-R Recommendation T.81 (09/92) Information technology -Digital compression and coding of continuous-tone still images -Requirements and guidelines
- (18) MPEG2
 - ISO/IEC 13818-1:1996 Information technology Generic coding of moving pictures and associated audio information: Systems
 - ISO/IEC 13818-2:1996 Information technology Generic coding of moving pictures and associated audio information: Video
 - ISO/IEC 13818-3:1998 Information technology Generic coding of moving pictures and associated audio information Part 3: Audio
 - ITU-T Recommendation H.222.0 (07/95) Information technology -Generic of moving pictures and associated audio information: Systems
 - ITU-T Recommendation H.262 (07/95) Information technology -Generic of moving pictures and associated audio information: Video
- (19) MPEG4
 - ISO/IEC 14496-1:1999 Information technology -- Coding of audio-visual objects -- Part 1: Systems
 - ISO/IEC 14496-2:1999 Information technology -- Coding of audio-visual objects -- Part 2: Visual

(20) PER

- JIS X 5606-2:1998 Information technology ASN.1 encoding rules -Part 2: Specification of Packed Encoding Rules (PER) (ISO/IEC 8825-2:1996 Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER))
- (21) PPP
 - RFC 1661 The Point-to-Point Protocol (PPP), W. Simpson, July 1994. (Status: STANDARD)
- (22) SNMP
 - RFC 1157 Simple Network Management Protocol (SNMP), J.D. Case, M. Fedor, M.L.Schoffstall, C. Davin, May-01-1990. (Status: STANDARD)
- (23) TCP
 - RFC 793 Transmission Control Protocol. J. Postel. Sep-01-1981. (Status: STANDARD)
- (24) TFTP
 - RFC 1350 THE TFTP PROTOCOL (REVISION 2), K. Sollins, July 1992. (Status: STANDARD)
- (25) UDP
 - RFC 768 User Datagram Protocol. J. Postel. Aug-28-1980. (Status: STANDARD)
- (26) V.24/V.28
 - ITU-T Recommendation V.24 (10/96) List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit terminating equipment (DCE)
 - ITU-T Recommendation V.28 (03/93) Electrical characteristics for unbalanced double current interchange circuits
- (27) X.21
 - ITU-T Recommendation X.21(09/92) Interface between Data Terminal Equipment Data Circuit - terminating Equipment for synchronous operation on public data network

4 Terms and Abbreviation

4.1 Terms and Definitions

Protocol Sets	Unit by which protocol specification of each layer is combined based on OSI basic reference model as a protocol rule applied to communication system of road manager. To be defined separately by each lower and by each upper layer.
Lower Layer	Generic name of physical layer and Datalink layer of OSI basic reference model
Upper Layer	Generic name to Network layer – Application layer of OSI basic reference model
Layer n	Abbreviation of each layer of OSI basic reference model Layer 7: Application Layer Layer 6: Presentation Layer Layer 5: Session Layer Layer 4: Transport Layer Layer 3: Network Layer Layer 2: Datalink Layer Layer 1: Physical Layer

4.2	Abbreviation	and	Definitions
-----	--------------	-----	-------------

ASN.1	Abstract Syntax Notation 1
ATM	Asynchronous Transfer Mode
BER	Basic Encoding Rules
CER	Canonical Encoding Rules
DATEX-ASN	the Data Exchange Protocol in ASN.1
DER	Distinguished Encoding Rules
DSRC	Dedicated Short Range Communication
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union –
	Telecommunication Standardization Sector
LAN	Local area Network
M-JPEG	Motion Joint Photographic Expert Group
MPEG2	Moving Picture Expert Group 2
MPEG4	Moving Picture Expert Group 4
OSI	Open System Interconnection
PER	Packed Encoding Rules
PPP	Point to Point Protocol
SNMP	Simple Network Management Protocol
RFC	Request For Comments
ТСР	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
WAN	Wide area Network

5 Protocol

5.1 Protocol Set

5.1.1 Lower Layer Protocol Set

(1) Network Model

Figures 5.1-1 and 5.1-2 illustrate the network model to which this standard is to be applied. Figure 5.1-1 shows the network model of dedicated network, and Figure 5.1-2 shows the network model of public network.

Transmission equipment for dedicated network is the terminal determined in "No. 42 Digital Transmission Equipment (SDH)" issued by the Ministry of Land, Infrastructure and Transport. An Optical Repeating Amplifier Installation might exist between Transmission Equipment.

The ITS systems shown in Section "Scope" in Chapter 2 shall be configured with the whole network model or a part of the network model. However, when a special equipment or device is used in the ITS system, the configuration may differ from this network configuration. In that case, this Standard may not be applied.



Figure 5.1-1: Network Model (Dedicated)



Figure 5.1-2: Network Model (Public Network)

(2) Protocol Set

Table 5.1-1 shows a lower layer protocol set for the wired and wireless system. The interface points $\textcircled{0}\sim\textcircled{8}$ in the table are illustrated in Figures 5.1-1 and 5.1-2.

Usage*1		,	WAN			LAN							
	2,8	3,6,7	3,6,7	3,7	1	4	5	9	5				
No. *2	#a	#b	#c	#d	#e	#f	#g	#h	#i	#j			
Layer 2	-	PPP	PPP	PPP	ATTN /	EDDI	Ethomast	Fast	Gigabit	DSRC-L2			
Layer 1	G.703a	I.430	I.431	X.21	AIM	FDDI	Einernet	Ethernet	Ethernet	DSRC-L1			

 Table 5.1-1: Lower Layer Protocol Set

*1 : Interface locations are shown Figure 5.1-1 and Figure 5.1-2. *2 : Interface Number of Lower Layer Protocol Set

16

5.1.2 Upper Layer Protocol Set

The protocol usage is classified into the following six categories according to the ITS systems as described in section "Scope" in Chapter 2.

- Motion Picture Transfer
- File Transfer
- Data Transfer *1
- Roadside Control
- Open Access
- Roadside-to-vehicle

Table 5.1-2 shows the Upper Layer Protocol Set applied to these six groups.

*1 : "Data Transfer" shown here means the transmitting information defined by message sets and data sets as electronic transmissions between equipment located among various centers or located between centers and roadsides, without generating files.

Table 5. 1.2-1 shows how Datex-ASN is applied as a protocol of Layer 7 (application layer). However, since Datex-ASN is currently under consideration to be adopted as an ISO standard, it is explained in 6.1.

Usage			Motion	Picture	Transfe	er		File T	ransfer	Data Tr	ransfer ^{*1}	*2	Open Access	*3
No.* <mark>4</mark>	#1	#1-1	#1-2	#2-1	#2-2	#3	#4	#5	#6	#7* ⁵	#8* ⁵	#9	#10	#11
Layer 7	-	-	-			H.261	M-JPEG	FTP	TFIP	DATEX -ASN	DATEX -ASN	SNMP	HTTP	DSRC-L7
Layer 6	MPEG2	MPEG2	MPEG2	MPEG4	MPEG4					BER,CER, DER,PER	BER,CER, DER,PER			-
Layer 5	-	-	-							-	-			-
Layer 4	_	UDP	ТСР	UDP	ТСР	UDP	UDP	ТСР	UDP	UDP	ТСР	UDP	ТСР	-
Layer 3	-	IP	IP	IP	IP	IP	IP	IP	IP	IP	IP	IP	IP	-

Table 5.1-2: Upper Layer Protocol Set

*1: "Data Transfer" shown here means the transmitting information defined by message sets and data sets as electronic transmissions between equipment located among various centers or located between centers and roadsides, without generating files.

*2: Roadside Control

***3**: Roadside-to-vehicle (Dedicated Short Range Communication)

***4**: Number of Upper Layer Protocol Set

*5: DATEX-ASN includes File Transfer(#5,#6) in the process of data publication.

5.2 Protocol Set Combination

Table 5.2-1 shows the combination of protocol set of the lower and the upper layers. The combination is either "technically feasible" or "technically infeasible or under development".

Table 5.2-1 defines the available protocols in view of the technical aspect.

						Uppe	er Layer F	Protocol S	Sets					
Lower Layer			Motion	Picture 7	Transfer			File Transfer		Data T	ransfer	*1	Open Access	Road- Vehicle
Protocol Sets	#1 (MPEG2)	#1-1 (MPEG2/ UDP/IP)	#1-2 (MPEG2/ TCP/IP)	#2-1 (MPEG4/ UDP/IP)	#2-2 (MPEG4/ TCP/IP)	#3 (H.261/ UDP/IP)	#4 (M-JPEG /UDP/IP)	#5 (FTP/ TCP/IP)	#6 (TFTP/ UDP/IP)	#7 (DATEX -ASN/ UDP/IP)	#8 (DATEX -ASN/ TCP/IP)	#9 (SNMP/ UDP/IP)	#10 (HTTP/ TCP/IP)	#11 (DSRC -L7)
#a (G.703a)	0	×	×	×	×	×	×	×	×	×	×	×	×	×
#b (Leased Line, ISDN ~192kb/s PPP)	×	×	×	0	0	0	0	0	0	0	0	0	0	×
#c (Leased Line,ISDN ~1.5Mb/s PPP)	×	×	×	0	0	0	0	0	0	0	0	0	0	×
#d (Leased Line PPP)	×	0	0	0	0	0	0	0	0	0	0	0	0	×
#e (ATM)	×	0	0	0	0	0	0	0	0	0	0	0	0	×
#f (FDDI)	×	0	0	0	0	0	0	0	0	0	0	0	0	×
#g (Ethernet)	×	0	0	0	0	0	0	0	0	0	0	0	0	×
#h (Fast Ethernet)	×	0	0	0	0	0	0	0	0	0	0	0	0	×
#i (Gigabit Ethernet)	×	0	0	0	0	0	0	0	0	0	0	0	0	×
#j (DSRC-L1,l2)	×	×	×	×	×	×	×	×	×	×	×	×	×	0

Table 5.2-1: Technical feasibility in terms of Protocol Set Combinations

Explanatory notes O: technically feasible, ×: technically infeasible

*1: Roadside Control

6 Protocol Detail

This chapter describes the protocols other than de facto standards in detail.

6.1 DATEX-ASN

6.1.1 DATEX-ASN Protocol Detail

(1) Summary

DATEX-ASN prescribes Layer 7 Protocol between centres for Transport Information and Control Systems (TICS). It is under the standardization process in ISO. It is not limited to the ITS application, but can be applied to general systems.

DATEX-ASN prescribed by this standard is based on ISO/WD 14827-2 v20. With regard to its use in Japan's ITS system, some additions have been made to 14827-2 v20. The following items are prescribed in DATEX-ASN protocol of this standard.

- Data exchange procedure
- Application session
- Data request
- Data response
- Message sequence
- State transition
- Data Packet Structures

Message sequence, State transition and Data Packet Structures are discussed in Sections 6.1.2, 6.1.3 and 6.1.4.

(2) Data Exchange Procedure

DATEX-ASN is a protocol for the communication between-with two systems, one for a client and the other for a server. An application session is established, on which data packets and files are exchanged.

File exchange is done by a file transfer protocol procedure through a port that is separate from the application session.

1) Data Packet

Data transmission between applications is all done with data packets shown in the followings.

Generally, the Application Protocol Data Unit (APDU) is divided into the Application Service Header and the Application Service Data Unit (ASDU). The Application Service Header, which contains data related to the messaging infrastructure, is related to the protocol defined in this standard, while ASDU, which contains data that is going to be processed by the participating systems, is related to the message set standard.

Note that DATEX-ASN data packet itself includes the ASDU area as well as Application Service Header.



Figure 6.1-1: Data packet structure

Table 6-1-1 shows a table of data packet items.

No	Name of Item	Summary	Notes
1	Version number	DATEX-ASN version number	
2	Authenticated data	Authenticated data between client/server.	
3	Data packet number	Numbers assigned sequentially from 1 for exchange of data packets between client/server.	
4	Data packet priority	Priority of message.	
5	Header option	Protocol header. Data collection source, destination, destination domain name and address.	
6	CRC number	Message byte stream for error checking.	
7	PDU ^{*1}	See Table 6.1-2	

 Table 6.1-1: Table of data packet items

*1: This PDU is not a PDU that is defined by ISO but it is named individually by DATEX-ASN.

No	Name of PDU	Summary	Notes
1	Initiate	For server to prompt client to request a login.	
2	Login	For client to request establishment of application session.	
3	FrED	For response not accompanying acceptance or rejection. Used for maintaining application session, for client to request termination of application session (logout), for client response to ending file reception.	
4	Terminate	For server to prompt client to request a logout.	
5	Logout	For client to request termination of application session.	
6	Subscription	For client to request data. For server to specify data response method (data packets or file transfer protocol) and content of data to be requested.	
7	Publication	For data response from server. If client requests data response by data packets, the response will have an application message set in the end application message section of the data packets. For a file transfer protocol response, the response is the name of file to be transferred.	
8	Transfer Done	For client to acknowledge data response by file transfer from server by sending end of reception.	
9	Accept	For positive response by server or client to each request (Initiate, Login, Terminate, Subscription, Publication) from client or server.	
10	Reject	For negative response by server or client to each request (Initiate, Login, Terminate, Subscription, Publication) from client or server.	

Table 6.1-2: PDU List

2) Application Session

An application session must be set up for communication between systems (between applications).

By setting up an application session, one side, the logon side, becomes the client and the other becomes the server.

The application session is a one way link (data request from client only) and the data is transmitted one way from the server to the client.

Therefore, for bi-directional data transfer between applications, another application session must be set up with client and server roles reversed.

3) Layer 6 and lower protocols

Layer 6 and lower protocols shall be in accordance with Chapter 5. However, the same protocols shall be used during one application session.

4) **Response timeout time**

Client and server shall set adequate response timeout times with due consideration for network transfer delays and application processing times, and shall exchange response times with respect to the application session.

5) Port number

The initial port number shall be 355.

- (3) Establish/Maintain/Terminate Application Session
- 1) Establishment of Application Session

The establishment of an application session begins with a request from the client to establish a session ('login' request) but a request from the server is also possible.

In the case of a request from the server, an 'initiate' request is issued asking the client to issue a request to establish a session ('login' request).

The server receives the request from the client to establish a session ('login' request), checks the whether the request is appropriate and sends an 'accept' or 'reject' response to the client. However, there may be no response if the server judges that there is a security problem.





Figure 6.1-2: Procedure for establishing an application session

2) Maintenance of Application Session

The application session is maintained by a "friendly exchange of data" (FrED) between server and client to confirm each other's presence.

This FrED exchange is done from the client and unless there it is done within a certain time after the Login request, the application session is terminated.

Figure 6.1-3 shows the procedure for maintaining an application session.



Figure 6.1-3: Application session maintenance procedure

3) Termination of Application Session

The termination of application session begins with a request from the client to terminate a session ('logout' request) but a request from the server is also possible.

In the case of a request from the server, an 'terminate' request is issued asking the client to issue a request to terminate a session ('logout' request).

If there is no response from the client to a terminate request within a certain time, the request is repeated and if there is still no response, the application session is terminated at that point.

Figure 6.1-4 shows the procedure for terminating an application session.



Figure 6.1-4: Procedure for terminating an application session

If the client, while requesting data, stops that request and terminates the application session, the data request must be cancelled and the application session terminated.

However, in the case that the data request continues even after termination of the application session, the application session can be terminated without canceling the data request.

(4) Data request

For a data request, the client specifies the required items in a request data packet ("subscription"), to which the server responds with "accept" or "reject" depending on whether a data response will be made.

Table 6.1-3 shows data request items to be specified by the client and Figure 6.1-5 shows the data request procedure.

No	Main items specified	Summary	Notes
1	Serial-nbr	Sequence of data request numbers for one Client/Server unit. This number can be used if a data request is to be amended or canceled and to establish correspondence with data responses from the server.	
2	Persistent-bool	Whether this data request is valid even after termination of application session	
3	Status-cd	To distinguish New/Update/Cancel data request.	
4	Mode	To distinguish New/Update/Cancel data request.	
5	PublishFormat-cd	Data response method (file transfer FTP/TFTP/data packets)	
6	Priority-cd	Response priority	
7	Guarantee-bool	Specification guaranteed delivery (Client reply or no reply with FrED for data response from Server).	
8	CancelReason-cd	Reason if Status-cd is "Cancel"	
9	EndApplication-Message	Message set. This message set must be in accordance with Road Communication Standards for message sets.	

Table 6.1-3: Table of data request items



Figure 6.1-5: Data request procedure

- (5) Data Response
- 1) Data response by data packet

If "response by data packet" from the client is specified in the data request, the server will respond to the data request from the client by sending in a "publication" message.

The client will respond to data received with "accept" or "reject".

Figure 6.1-6 shows the procedure for data response by data packet.



Figure 6.1-6: Procedure for data response by data packet

2) Data response by file transfer

If "response by file transfer" from the client is specified in the data request, the server responds to the data request from the client with a data response notification ("publication" message) advising the name of the file to be transferred. The client checks whether the data can be received according to the contents of the notification and responds with "accept" or "reject".

On receiving "accept", the server transfers the file through a different port by file transfer protocol.

When the file has been received, the client issues 'transfer-done' and the server responds with 'FrED', which completes one sequence of the data response, but if the content of the received file is wrong, the client will issue 'reject'.



Figure 6.1-7: Procedure for data response by file transfer

6.1.2 DATEX-ASN Message Sequence

Here we indicate the sequence of DATEX-ASN messages. The various timers are as shown below.

- Tc1: The timer that waits for a response when the client requests the session establishment and the session termination.
- Tc2: The timer that waits for a response when the client requests information and issues file reception completed message.
- Tc3: The timer for the period for the client to issue a request for the session to be maintained.
- Tc4: Timer used to maintain a session on the client side.
 - A timeout on this timer is taken to be an abnormality on the server side.

Value is set to at least 3 times Tc3.

- Ts1: The timer that waits for a response when the server issues an initiate and terminate request.
- Ts2: The timer that waits for a response to a notification of information from the server side
- Ts3: Timer used to maintain a session on the server side
- (1) Establishment of application session
- 1) Normal sequence

Figure 6.1-8 shows the normal sequence of application session establishment.



Figure 6.1-8: Normal sequence of application session establishment

2) Abnormal sequence of initiate request response Figure 6.1-9 indicates an abnormal response sequence to a request to initiate application session establishment.



Figure 6.1-9: Abnormal sequence of application session establishment (Initiate request response abnormal)

3) Abnormal sequence of login request response Figure 6.1-10 indicates an abnormal response sequence to a request for application session establishment.



Figure 6.1-10: Abnormal sequence of application session establishment (Establishment request response abnormal)

(2) Maintenance of application session

1) Normal sequence

Figure 6.1-11 shows the normal sequence of application session maintenance.



Figure 6.1-11: Normal sequence of application session maintenance

2) Abnormal sequence when server is faulty

Figure 6.1-12 indicates an abnormal sequence when the application session maintenance server is faulty.



Figure 6.1-12: Abnormal sequence of application session maintenance (Server fault)

3) Abnormal sequence when client is faulty Figure 6.1-13 indicates an abnormal sequence when the application session maintenance server is faulty.



Figure 6.1-13: Abnormal sequence of application session maintenance (Client fault)

- (3) Termination of application session
- 1) Normal sequence

Figure 6.1-14 shows a normal application session termination sequence.



Figure 6.1-14: Normal of sequence application session termination

2) Abnormal terminate request and response sequence Figure 6.1-15 shows an abnormal terminate request and response sequence for an application session termination.



Figure 6.1-15: Abnormal sequence of application session termination (Abnormal terminate request and response)

3) Abnormal session terminate request and response sequence Figure 6.1-16 shows an abnormal session terminate request and response sequence for an application session termination.



Figure 6.1-16: Abnormal sequence of application session termination (Abnormal session terminate request and response)

(4) Data request

1) Normal sequence

Figure 6.1-17 shows a normal request sequence from the client.



Figure 6.1-17: Normal data request sequence

2) Abnormal sequence

Figure 6.1-18 shows an abnormal data request sequence from the client.



Figure 6.1-18: Abnormal data request sequence

(5) Data response

1) Normal sequence

Figure 6.1-19 shows a normal data response sequence.



Figure 6.1-19: Normal data response sequence

In the above figure, if the client rejects a file transfer, the server observes with Ts2 timer but no error is issued even if there is no response within the specified time. Also, a "reject" received after Ts2 timer stops will be ignored.

2) Abnormal data message response sequence Figure 6.1-20 shows an abnormal data message response sequence.



Figure 6.1-20: Abnormal data response sequence (Abnormal data message response)

3) Abnormal transfer-done response sequence Figure 6.1-21 shows an abnormal transfer-done response sequence.



Figure 6.1-21: Abnormal data response sequence (Abnormal transfer-done response sequence)

(6) Examples of complete sequences

The exchange of data between client and server is based on the sequences shown above but the following are examples of "simple" and "continuous" data requests from the client.

1) A "Simple" example

Figure 6.1-22 shows an example of non-continuous data acquisition by the client from the server.

In this case, response is by data packet. Also, application session maintenance has been omitted.



Figure 6.1-22: A "Simple" example

In the example above, application session termination is not necessary if further data requests are to be made. 2) A "Continuous" example

Figure 6.1-23 shows an example of continuous data acquisition by the client from the server.

In this example, the client makes a data request and temporarily terminates the application session, then waits for a data response from the server.



Figure 6.1-23: A "Continuous" example

6.1.3 State Transition

State transition tables of DATEX-ASN client and server are shown by Table 6.1-4 and 6.1-5.

Event				Request from A	oplication				Messae	e received from	ıServer				Т	imeaut		
Status		Request for session establishmen t	Request for data	Response to data notification	Termination of file reception	Request for session termination	Request for initialization	Response to session establishmen t request	Response to request for data	Notification of data	Response to termination of file reception	Response to maintaining session	Request for termination	Response to session termination request	Tc1 timeout	Tc2 timeout	Tc3 timeout	Tc4 timeout
	\sim	El	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13	E14	E15	E16	E17
Idle (session un established)	S1	•Issue request to establish connection •Start Tc1 \$\$3	•Error response →S1	•Error response	•Error response	•Error response →S1	•NotifyAP	•Cancel	•Cancel 	•Cancel	•Cancel	•Cancel →St	•Cancel	•Cancel				
Establishin g session (Accepting initializatio n request)	82	•Issue request to establish session •Start Tc1	•Error response	•Error response	•Error response	•Error response	•NotifyAP	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel				
Establishin g session (Requestin g establish-m ent)	8	•Error response	•Error response	•Error response	•Error response	•Error response	•Cancel		•Cancel	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel	•Notify AP •Stop Tc1			
				→\$ 3			-→\$3	© \$4 ©- -\$1		-→\$3		→ \$3	-→\$3		→ \$1			
Establishin g session	S4	•Error response	•Issue data request •Start Tc2	•Issue data notificatio n response	•Issue terminatio nof file reception •Start Tc2	•Issue request to terminate session •Start Tc1	•Cancel	•Cancel	•NotifyAP •Stop Tc2	•Notify AP	•NotifyAP •Stop Tc2	•Reset Tc4	•NotifyAP	•Cancel		•NotifyAP •Stop Tc2	•Issue response to maintain session •Start Tc3	•NotifyAP •Stop timers
		→ \$4	→\$ 4	→\$4	→\$4	→\$6	→\$ 4	→ \$4	→\$ 4	→\$ 4	→\$ 4	→\$4	→ \$5	→\$ 4		→ \$4	→\$ 4	→S1
Handling terminatio n request	S5	•Error response	•Error response	•Error response	•Error response	•Issue request to terminate session •Start Tc1	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel				
		→ \$5	→\$ 5	→ \$5	→ \$5	→\$6	→S 5	→ \$5	→ \$5	→ \$5	→ \$5	→ \$5	→ \$5	→\$ 5				
Awaiting response to terminate session	S6	•Error response	•Error response	•Error response	•Error response	•Error response	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel	•Notify AP •Stop Tc1	•Notify AP •Stop Tc1			
		→\$6	→S 6	→\$6	→S 6	→\$6	→\$6	→\$6	→\$6	→\$6	→S 6	→\$6	→\$6	→S1	→S1			

Table 6.1-4: DATEX-ASN State Transition Table (Client)

	_																
Event				Reque	est from Applica	tion					Message recei	ved from Client				Timeout	
Status		Request for initialization	Response to request to establish session	Response to request for data	Notification of data	Response to termination of file reception	Request for termination	Response to session termination request	Request to establish session	Request for data	Response to data notification	Terminate file reception	Request to maintain session	Request to terminate session	Ts1 timeout	Ts2 timeout	Ts3 timeout
		E1	E2	E3	E4	E5	E6	Ē7	E8	E9	E10	E11	E12	E13	E14	E15	E16
Idle (session un established)	S1	•Issue initializati on request •Start Ts1	•Error response	•Error response	•Error response	•Error response	•Error response	•Error response	•Notify AP	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel			
		→S2	→S1	→S1	→S1	→S1	→S1	→S1	→S3	→S1	→S1	→S1	→S1	→S1			
Establishin g session (Requestin	S2	•Error response	•Error response	•Error response	•Error response	•Error response	•Error response	•Error response	•Notify AP •Stop Ts1	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel	•Notify AP •Stop Ts1		
g initializatio n)		→S2	→S2	→S2	→S2	→S2	→S2	→S2	→S3	→S2	→S2	→S2	→S2	→S2	→S1		
Establishin g session (Accepting establish-m ent request)	S3	•Error response	 Accept Issue response (acceptance) to request for establishing session Start Ts3 Reject Issue response (rejection) to request for establishing session 	•Error response	•Error response	*Error response	•Error response	•Error response	•Cancel	*Cancel	*Cancel	*Cancel	*Cancel	•Cancel			
		→S3	©→S4 ②→S1	→S3	→S3	→S3	→S3	→S3	→S3	→S3	→S3	→S3	→S3	→S3			
Establishin g session	S4	•Error response	•Error response	•Issue response to request for data	•Issue data notification •Start Ts2	•Issue response to terminatio n of data reception	•Issue terminatio n request •Start Ts1 •Reset C1	•Error response	•Cancel	•Notify AP	•Notify AP •Stop Ts2	•Notify AP	•Issue response to maintainin g session •Reset Ts3	•Notify AP		•Notify AP •Stop Ts2	•Notify AP •Stop timer
		→S4	→S4	→S4	→S4	→S4	→S5	→S4	→S4	→S4	→S4	→S4	→S4	→ <mark>S6</mark>		→S4	→S1
Session terminatio n request in progress	S5	•Error response	•Error response	•Error response	•Error response	•Error response	•Error response	•Error response	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel	•Notify AP			
		→S5	→S5	→S5	→S5	→S5	→S5	→S5	→S5	→S5	→S5	→S5	→S5	→S6	00→S5 ©→S1		
Handling request for session terminatio n	S6	•Error response	•Error response	•Error response	•Error response	•Error response	•Error response	•Issue response to terminate session •Stop timers	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel	•Cancel			
		->56	→ 5 0	->56	->56	I→56	->56	->SI	→ 5 6	->>6	I→56	I→56	->56	→56	1		

 Table 6.1-5: DATEX-ASN State Transition Table (Server)

Appendix: DATEX-ASN Packet Details

Details of DATEX-ASN packets are shown on the following pages.

DATEX-ASN Data Packet Structures (1/11)

D	Data Packet Structures	Name	Details
A.1 General			
RcsDatex-asnDataPacketStructure DEF	INITIONS AUTOMATIC TAGS ::= BEGIN		
DatexDataPacket ::= SEQUENCE {			
datex-Version-cd	ENUMERATED {	Version number	-Indicates DATEX-ASN version.
	experimental,		0: Experimental
	version-1		1: Version 1 (=This version)
	},		-This version dose not accord with the version of Road Communication
			Standards.
datex-Data-txt	C2CAuthenticatedMessage,	Message data	-C2C authenticated message
an optionally encrypted C2	2CAuthenticatedMessage		-Refer to C2CAuthenticatedMessage discussed below
datex-Crc-id	OCTET STRING (SIZE (2))	CRC number	-Message byte stream for error checking
			-Application of CRC algorithm prescribed by ISO3309
}			
C2CAuthenticatedMessage ::= SEQUE	NCE {	Authenticated message	
datex-AuthenticationInfo-txt	OCTET STRING (SIZE (0255)),	Authenticated data text	-Authenticated data agreed between two systems (client and server)
datex-DataPacket-nbr	INTEGER (04294967295),	Data packet number	-Numbers assigned from 0 in units established by the session
			-Packets transmitted by C/S during the session begin with zero and are then
			incremented by 1.
datex-DataPacketPriority-cd	INTEGER (110),	Data packet priority number	-Priority grading of message (1~10)
			-Messages with the same priority must be handled in the order in which they
			are received but a higher priority message can be handed before one of
			lower priority.
options	HeaderOptions,	Header options	-Refer to HeaderOptions discussed below
pdu	PDUs	Protocol data units	-Refer to A2 (Protocol Data Unit) discussed below
}			

Data	a Packet Structures		Name	Details
HeaderOptions ::= SEQUENCE {			Header options	
datex-Origin-txt	UTF8String (SIZE (040))	OPTIONAL,	Collection source	-Domain name of system collecting data contained in message
				Not used in Road Communication Standards
datex-OriginAddress-loc	OCTET STRING	OPTIONAL,	Address of collection source	-Address of data collecting system
				Not used in Road Communication Standards
				-Naming criteria are as follows:
				VALUE RULE "AddressCode ::= CHOICE
				{
				gis IMPLICT [1] NUMERIC STRING
				MhORName IMPLICT [2] MhORName,X.500
				dn IMPLICT [3] DistinguishedName,X.500
				IsdnOrPhonenumber IMPLICT [4] E164Form
				rfc822Address IMPLICT [5] PRINTABLESTRING
				pstnAddress IMPLICT [6] NUMERIC STRING}
				}"
datex-Sender-txt	UTF8String (SIZE (040))	OPTIONAL,	Sender	-Domain name of sending system
datex-SenderAddress-loc	OCTET STRING	OPTIONAL,	Address of sender	-Address of sending system
				-Naming criteria are same as for collection origin address
datex-Destination-txt	UTF8String (SIZE (040))	OPTIONAL,	Destination	-Domain name of destination system
datex-DestinationAddress-loc	OCTET STRING	OPTIONAL,	Destination address	-Address of destination system
				-Naming criteria are same as for collection origin address
cost	Cost	OPTIONAL,	Cost	-Refer to Cost discussed below
datex-DataPacketTime	Time	OPTIONAL	Time data packet created	-Time this data packet was created
}				
Cost ::= SEQUENCE {			Cost	-Cost expressed by currency code, factor and quantity
				e.g. Currency code: dollar, Factor: 3 (10 ⁻³), Quantity: $11 \rightarrow 0.011$ dollars
amount-Currency-cd	OCTET STRING (SIZE (3)),		Currency code	-Cost currency code (conforms to ISO4217)
amount-Factor-qty	INTEGER,		Factor	-Factor (n of 10 ⁻ⁿ)
amount-Quantity-qty	INTEGER		Quantity	-Quantity
}				

DATEX-ASN Data Packet Structures (2/11)

Data Pa	acket Structures	Name	Details
A.2 Protocol Data Unit		Protocol data unit	
PDUs ::= CHOICE { initiate login fred terminate logout subscription publication transfer-done accept reject }	Initiate, Login, FrED, Terminate, Logout, Subscription, Publication, TransferDone, Accept, Reject		-Data packet indicated below 0: initiate 1: log-in 2: Fred 3: terminate 4: logout 5: subscription 6: publication 7: transferDone 8: accept 9: reject
A.3 Initiate Data packet Structure		Initiate data packet	
Initiate ::= SEQUENCE { datex-Sender-txt datex-Destination-txt }	UTF8String (SIZE (040)), UTF8String (SIZE (040))	Sender Destination	-Domain name of sending system (server side) -Domain name of destination system (client side)
A.4 Login Data packet Structure		Login data packet	
Login ::= SEQUENCE {			
datex-Sender-txt	UTF8String (SIZE ((040)),	Sender	-Domain name of sending system (server side)
datex-Destination-txt	UTF8String (SIZE (040)),	Destination	-Domain name of destination system (client side)
datexLogin-UserName-txt	OCTET STRING,	Username	-ID of user requesting login
datexLogin-Password-txt	OCTET STRING,	Password	-Password of user requesting login -User ID and password are checked by the application
datexLogin-EncodingRules-id	SEQUENCE OF OBJECT IDENTIFIER,	Encoding rules	-Indicates encoding rules.
datexLogin-HeartbeatDurationMax-qty	INTEGER (065535),	FrED time	-FrED duration for conversion for heartbeat. (Seconds) -Indicates no heartbeat if set to zero
datexLogin-ResponseTimeOut-qty	INTEGER (0255),	Timeout time	-Timeout time for response to transmission. (Seconds) -Value common to both client and server.
datexLogin-Initiator-cd	ENUMERATED { serverInitiated, clientInitiated, }	Initiator	-Indicates source of login request 0: Server (login by request initiated from server side) 1: Client
uatexLogin-DatagramSize-qty	INTEGER (005555) DEFAULT 5/6,	waxinum datagram length	-waximum uatagram length for this session

DATEX-ASN Data Packet Structures (3/11)

DATEX-ASN Data Packet Structures (4/11)

Data Pao	cket Structures	Name	Details
A.5 FrED Data packet Structure		FrED data packet	
FrED ::= INTEGER (04294967295)	- datexFrED-ConfirmPacket-nbr		-Set to 0 for FrED for heartbeat -For FrED for other than heartbeat, set the data package number (as determined by A1) that is the object of this FrED
A.6 Terminate Data packet Structure		Terminate data packet	
Terminate ::= ENUMERATED { other, serverRequested, clientRequested, serverShutdown, clientShutdown, serverCommProblems, clientCommProblems, } }	- datexTerminate-Reason-cd	Reason for termination request	 -Indicates reason for requesting termination of session 0: Other 1: Requested by server 2: Requested by client 3: Server shutdown 4: Client shutdown 5: Communication problem on server side 6: Communication problem on client sided -Other than above shall be determined at installation time
A.7 Logout Data packet Structure		Logout data packet	
Logout ::= ENUMERATED { other, serverRequested, clientRequested, serverShutdown, clientShutdown, serverCommProblems, clientCommProblems, }	- datexLogout-Reason-cd	Reason for logout	-Indicates reason for logout request (same as Termination request)
A.8 Subscription Data packet Structure		Subscription data packet	
Subscription ::= SEQUENCE {			
datexSubscribe-Serial-nbr	INTEGER (04294967295),	Subscription number	-Sequence of requests for data from client (1~) -Used for new data requests. Use former subscription number for updates or cancellations. -Assigned sequentially from one client/server sequence. (If one client has established sequences with several servers, there is a sequence for each.)
type	SubscriptionType,	Subscription type	-Refer to SubscriptionType mentioned below
}			

Data	Packet Structures	Name	Details
SubscriptionType ::= CHOICE {		Subscription type	
subscription	SubscriptionData,	SubscriptionData	-Refer to SubscriptionData mentioned below
datexSubscribe-CancelReason-cd	ENUMERATED { other,	Reason for subscription cancellation	-Indicates reason for canceling Subscription. 0: Other
	dataNotNeeded,		1: Data not needed
	errorsInPublication,		2: Faulty response details
	pendingLogout,		3: Cancelled with end of session
	processingMgmt,		4: Processing management (cancelled for resources reasons)
	bandwidthMgmt,		5: Band width management (cancelled due to another priority
	-		subscription)
	}		-Other than above shall be determined at installation time
}			
SubscriptionData ::= SEQUENCE {		Subscription data	
datexSubscribe-Persistent-bool	BOOLEAN,	Continuous setting	-Indicates whether this subscription will remain valid after the session is
			terminated.
			-0 (valid) / 1 (invalid)
datexSubscribe-Status-cd	ENUMERATED {	Subscribe status	-Indicates new/update/cancel subscribe status
	new,		0: New
	update,		1: Update
	},		
mode	SubscriptionMode,	Subscription mode	-Refer to SubscriptionMode mentioned below
datexSubscribe-PublishFormat-cd	ENUMERATED {	Set reponse format	-Indicates request for form of data response format from server.
	other,		0: Other (not used for Road Communication Standards)
	ftp,		1: Response by FTP
	tftp,		2: Response by TFTP
	dataPacket,		3: Response by data packet (A9)
	},		
datexSubscribe-Priority-cd	INTEGER(110),	Response priority	-Indicates priority of response from server (10 levels 1 to 10)
			1 is highest, 10 is lowest.
datexSubscribe-Guarantee-bool	BOOLEAN,	Assured bool	-Indicates whether public access to response is requested
			-0 (True) / 1 (False)
message	EndApplicationMessage	End application message	-Application message for requesting data.
			-Refer to EndApplicationMessage discussed below
}			

DATEX-ASN Data Packet Structures (5/11)

Data Pa	cket Structures		Name	Details
SubscriptionMode ::= CHOICE { single event-driven periodic }	NULL, Registered, Registered		Subscription mode	-Indicates whether this is a single or a continuous subscription (event-driven/periodic) -No setting if single. -If continuous, described hereafter as Registered,
Registered::= CHOICE {			Continuously registered data	-Set in cases where subscription mode is "continuous"
continuous	SEQUENCE {		Continuous (periodic) setting	-If continuous is specified at start time and end time
datexRegistered-UpdateDelay-qty 0 means as soon as possib	INTEGER (04294967295) ole	DEFAULT 0,	Update (response) period	 -If event-driven, response time from occurrence of an event is specified in seconds. -If periodic, period is specified in seconds. -Initial value is 0, meaning "as soon as possible"
datexRegistered-StartTime defaults to immediate	Time	OPTIONAL,	Start time	-Indicates start time for request (continuous request). -Set in the Time format mentioned below. -0 means "start immediately". -A time requested before this request becomes "immediate".
datexRegistered-EndTime defaults to "until cancelled"	Time	OPTIONAL	End time	-Indicates end time for request (continuous request). -Set in the Time format mentioned below. -0 means "until this subscription is cancelled".
daily	SEQUENCE {		Date setting	-When setting Continuous in terms of days
datexRegistered-UpdateDelay-qty 0 means as soon as possible	INTEGER (04294967295)	DEFAULT 0,	Update (response) period	-Response time from the time an event occurs is specified in seconds. -Initially 0, meaning "as soon as possible".
datexRegistered-DaysOfWeek-cd	BIT STRING { other(0), Sunday(1), Monday(2), Tuesday(3), Wednesday(4), Thursday(5), Friday(6), Saturday(7)} (SIZE (8)),		Setting the day of the week	-Setting days of the week. 0: Other (every day) 1: Sunday 2: Monday 3: Tuesday 4: Wednesday 5: Thursday 6: Friday 7: Saturday

DATEX-ASN Data Packet Structures (6/11)

DATEX-ASN Data Packet Structures (7/11)

Data l	Packet Structures		Name	Details
datexRegistered-StartDate	Time	OPTIONAL,	Start date	-Either StartDate + StartTime + EndDate or StartDate + StartTime +
defaults to immediate				ContinuousTime are specified as a group
datexRegistered-EndDate	Time	OPTIONAL,	End Date	But,
defaults to "until cancelle	ed"			-Omission of StartDate means "immediate"
datexRegistered-StartTime	Time	OPTIONAL,	Start Time	-Omission of StartTime means midnight
defaults to midnight				-Omission of EndDate means "until cancelled"
datexRegistered-Duration-qty	INTEGER (065535)	OPTIONAL	Duration	-If both EndTime and ContinuousTime are omitted, an analysis
defaults to 1440 (i.e., 24	hours)			with EndDate omitted will have precedence.
}				-Duration is set in minutes. (e.g. 24 hours becomes 1,440)
}				-For expressing StartDate, EndDate and EndTime, refer to Time mentioned
				below.
Time ::= SEQUENCE {			Time setting	-Time setting
time-Year-qty	INTEGER (-3276832767)	OPTIONAL,	Year	-StartDate or EndDate settings are valid only when year, month, day and
defaults to current year unless otherw	vise specified			time zone are set.
time-Month-qty	INTEGER (112)	OPTIONAL,	Month	-Year, month, day are not needed for setting StartTime
defaults to current month unless othe	erwise specified			-Use 4-digit Western system for year
time-Day-qty	INTEGER (131)	OPTIONAL,	Day	-Month is 1~12
defaults to current day unless otherw	ise specified			-Day is 1~31
time-Hour-qty	INTEGER (023)	DEFAULT 0,	Hour	-Hour is 0~23
time-Minute-qty	INTEGER (059)	DEFAULT 0,	Minute	-Minute is 0~59
time-Second-qty	INTEGER (059)	DEFAULT 0,	Second	-Second is 0~59
secondFractions	CHOICE {		Second fractions	-For setting less than q second, select from 1/10, 1/100, 1/1000
time-Deciseconds-qty	INTEGER (09),		1/10 seconds	If it is necessary to specify less than 1/10000, set this at installation time.
time-Centiseconds-qty	INTEGER (099),		1/100 seconds	- Time zone is the difference in hours from International standard time
time-Milliseconds-qty	INTEGER (0999),		1/1000 seconds	(UTC) specified in hours (-15 to 13) and minutes (0 to 59)
},		DEFAULT 0,		If omitted, year month, day default to present day
timezone	SEQUENCE {		Time zone	-If omitted, hour, minute, second default to 0,0,0
time-TimeZoneHour-qty	INTEGER (-1313)	DEFAULT 0,	Time difference	If omitted, time zone defaulte to LITC
time-TimeZoneMinute-qty	INTEGER (059)	DEFAULT 0	Time difference (minutes)	-If offitted, time zone defaults to 01C
}		OPTIONAL		
defaults to UTC				
}				

DATEX-ASN Data Packet Structures (8/11)

Data Pa	acket Structures	Name	Details
A.9 Publication Data Packet Structure		Publication data packet	
Publication ::= SEQUENCE {			
datexPublish-Guaranteed-bool	BOOLEAN,	Response guaranteed	-Indicates whether public access to response is guaranteed. -0 (True) / 1 (False)
format	Publish-Format	Response format	-Refer to publish-Format mentioned below
}			
Publish-Format ::= CHOICE {		Response format	
data	SEQUENCE OF PublicationData,	Response data	-Refer to PublicationData mentioned below
datexPublish-FileName-txt	UTF8String (SIZE (02000))	Response filename	-Filename for response due to file transfer
}			
PublicationData ::= SEQUENCE {		Response data	
datexPublish-SubscribeSerial-nbr	INTEGER (04294967295),	Subscription number	-Subscription number specified by the subscription data packet that is the source of this response
datexPublish-Serial-nbr	INTEGER (04294967295),	Publication number	-Serial numbers (1~) corresponding to the above Subscription numbers -Continuous responses are numbered sequentially from 1 with respect to the above Subscription numbers.
datexPublish-LatePublicationFlag-bool	BOOLEAN,	Response delay flag	-Indicates whether the update period set by the Subscription data packet that is the basis of this response was further delayed in transmission -0 (True : delay) / 1 (False)
publicationType	PublicationType	Response type	-Refer to PublicationType mentioned below
}	¥.		
PublicationType ::= CHOICE {		Response type	
datexPublish-Management-cd	ENUMERATED { TemporarilySuspended, Resume, terminate-other, terminate-dataNoLongerAvailable, terminate-publicationsBeingRejected, terminate-PendingShutdown, terminate-PendingShutdown, terminate-bandwidthMgmt, terminate-bandwidthMgmt, terminate-accessDenied, UnknownRequest, },	Response status	 -Indicates response status 0: Temporarily suspended 1: Resume 2: Terminate (other's request) 3: Terminate (data no longer available) 4: Terminate (publications being rejected) 5: Terminate (pending shutdown) 6: Terminate (processing management) 7: Terminate (bandwidth management 8: Terminate (access denied) 9: Terminate (unknown request) -Other than the above to be determined on installation
publicationData	EndApplicationMessage	Data	-Response message from application -Refer to EndApplicationMessage mentioned below
}			

DATEX-ASN Data Packet Structures (9/11)

Data P	acket Structures	Name	Details
EndApplicationMessage ::= SEQUENCE {		Application message	-Application message
endApplication-Message-id	OBJECT IDENTIFIER,	Message ID	-Object ID (including version number) of message set
endApplication-Message-msg	OCTET STRING	Message set	-Message set shall be in accordance with Road Communications Standards
			Message Set Standard. (Refer to Message Set Standard)
}			
A.10 Transfer Done Data packet Structure		TransferDone data packet	
TransferDone ::= SEQUENCE {			
datexTransferDone-FileName-txt	UTF8String (SIZE (02000)),	File name	-File name of received file
datexTransferDone-Success-bool	BOOLEAN	Successful reception bool	-Indicated whether reception was successful
		_	-0(True : success) / 1 (False : fail)
}			
A.11 Accept Data packet Structure		Accept data packet	
Accept ::= SEQUENCE {			
datexAccept-Packet-nbr	INTEGER (04294967295),	Response data packet number	-Indicates the number of this data packet for acceptance (as set by A1)
accept-Type	CHOICE {	Accept type	-Indicates the object to be accepted
datexAccept-Login-id	OBJECT IDENTIFIER,	Login	-For login response, set encoding rules specified by client
encoding rules			-For single Subscription, set margins
single-subscription	NULL,	Single Subscription	-For registered Subscription, set update (response) period specified by
datexAccept-Registered-nbr	INTEGER (04294967295),	Registered Subscription	client.
the accepted value for the Upda	teDelay parameter		-For Publication (positive response from client), set margins
publication	NULL	Publication	
}			
}			
A.12 Reject Data packet Structure		Reject data packet	
Reject ::= SEQUENCE {			
datexReject-Packet-nbr	INTEGER (04294967295),	Response data packet number	-Indicates the number of this data packet for rejection (as set by A1)
rejectType	RejectType,	Reject type	-Indicates object for rejection
			-Refer to RejectType mentioned below
alternateRequest	AlternateRequest OPTIONAL	Alternate request	-For a Subscription response, indicates the possible form of response
			(format that can accept a request as a Subscription)
			-For a specific format refer to AlternateRequest below.
}			

D	ata Packet Structures	Name	Details
RejectType ::= CHOICE {		Reject type	
datexReject-Login-cd	ENUMERATED {	Reason Login rejected	-Indicates reason for Login rejection
	other,		0: Other
	unknownDomainName,		1: Unknown domain name
	accessDenied,		2: Access denied
	invalidNamePassword,		3: Invalid password
	timeoutTooSmall,		4: Timeout too small
	timeoutTooLarge,		5: Timeout too large
	heartbeatTooSmall,		6: Heartbeat too small
	heartbeatTooLarge,		7: Heartbeat too large
	sessionExists,		8: Session exists
	maxSessionsReached,		9: Maximum sessions reached
	},		-Other than the above to be determined on installation
datexReject-Subscription-cd	ENUMERATED {	Reason Subscription	-Indicates reason for rejecting Subscription
		rejected	
	other,		0: Other
	unknownSubscriptionNbr,		1: Unknown Subscription number
	invalidTimes,		2: Invalid times
	frequencyTooSmall,		3: Update period too small
	frequencyTooLarge,		4: Update period too large
	invalidMode,		5: invalid mode
	publishFormatNotSupported,		6: invalid Publication format
	unknowSubscriptionMsgId,		7: unknown Subscription message ID
	invalidSubscriptionMsgId,		8: invalid Subscription message ID
	invalidSubscriptionContent,		9: invalid Subscription content
	},		-Other than the above to be determined on installation
datexReject-Publication-cd	ENUMERATED {	Reason for rejecting Publication	-Indicates reason for rejecting Publication
	other,		0: Other
	invalidPublishFormat,		1: Invalid Publication format
	},		-Other than the above to be determined on installation

DATEX-ASN Data Packet Structures (10/11)

Data Packet Structures		Name	Details
datexReject-PublicationData	SEQUENCE {	Publication data	-Content of response rejecting Publication
datexReject-SubscriptionSerial-nbr	INTEGER (04294967295),	Subscription number	-Subscription number and Publication number of data response that is
datexReject-PublicationSerial-nbr	INTEGER (04294967295),	Publication number	subject of this rejection
datexReject-PublicationData-cd	ENUMERATED {	Publication rejection	-Indicates contents of invalid Publication data format
	other,	types	0: Other
	unknownSubscription,		1: Unknown Subscription
	unknownPublicationNbr,		2: Unknown Publication number
	unknownPublicationMsgId,		3: Unknown message ID
	invalidPublicationMsgId,		4: Invalid message ID
	invalidPublicationMsgContent,		5: Invalid message content
	repeatedPublicationNbr,		6: Repeated Publication number
	},		-Other than the above to be determined on installation
}			
}			
AlternateRequest ::= SubscriptionType		Subscription type	-Same as previously mentioned A8(SubscriptionType)
END			