INTERNATIONAL STANDARD

ISO 14827-2

First edition
2005-11-01

Transport information and control systems — Data interfaces between centres for transport information and control systems —

Part 2: **DATEX-ASN**

Systèmes de commande et d'information des transports — Interfaces de données entre les centres pour systèmes de commande et d'information des transports —

Partie 2: DATEX-ASN

Reference number
ISO 14827-2:2005(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 2

3 Terms and definitions 3

4 Symbols and abbreviated terms 5

5 Implementation considerations 6

6 Data exchange procedures 6
6.1 General data packet procedures 7
6.2 General file procedures 7
6.3 Sessions 8
6.4 Requesting information 11
6.5 Publication of information 12

Annex A (normative) Data packet structures 16

Annex B (normative) Data dictionary 23

Annex C (normative) Value domains 45

Annex D (normative) DATEX-ASN over internet protocols 55

Annex E (normative) Protocol requirements list 56

Annex F (informative) Implementation guidance 61

Annex G (informative) Advantages of DATEX-ASN 62

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 14827-2 was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*, Working Group 9, with the collaboration of:

- European Road Transport Telematics Implementation Coordination Organization (ERTICO);
- Comité Européen de Normalisation (CEN);
- American Association of State Highway and Transportation Officials (AASHTO);
- Institute of Transportation Engineers (ITE);
- National Electrical Manufacturers Association (NEMA).

ISO 14827 consists of the following parts, under the general title *Transport information and control systems — Data interfaces between centres for transport information and control systems*:

- *Part 1: Message definition requirements*
- *Part 2: DATEX-ASN*

Introduction

In the 1980s and 1990s, transport networks became increasinigly congested and computer technologies were deployed to more efficiently manage the limited transport network. As these systems were deployed, it became more important to integrate nearby systems to properly provide the required services.

One of the first efforts to standardize the interface between transport control centres was a European Union effort led by the DATEX Task Force. In May 1993, this group was established as a horizontal activity to coordinate the diverging developments which were ongoing within the framework of the Advanced Transport Telematics (ATT) Programme. Within the ATT Programme, three different data exchange systems were developed: INTERCHANGE, EURO-TRIANGLE and STRADA. The group produced a set of basic tools to meet existing needs, including a common data dictionary, a common set of EDIFACT messages and a common geographical location referencing system.

The initial solution provided a common interface which satisfied the basic requirements of existing systems, and was named the Data Exchange Network (DATEX-Net) Specifications for Interoperability. During the initial efforts to deploy this International Standard, there was a growing sense that the message structure should be better organized and should be defined using Abstract Syntax Notation One (ASN.1) rather than EDIFACT.

ASN.1 presents a standard notation for the definition of data types and values. A data type is a class of information (e.g. numeric, textual, still image or video information). A data value is an instance of such a class. ASN.1 defines several basic types and their corresponding values, and rules for combining them into more complex types and values. These types and values can then be encoded into a byte stream according to any of several standardised encoding rules.

Efforts to standardize communications between transport control centres were also underway in other parts of the world. In 1997, all of these efforts began to merge, with the United States developing the initial draft of the ASN.1 structures for the Data Exchange in Abstract Syntax Notation (DATEX-ASN). These structures, called data packets, were then placed within a procedural context and submitted to the ISO standardization process.

A portion of the submittal dealt with the specification of messages. As this portion of the document could apply to various protocols, it was placed in ISO 14827-1 — *Message definition requirements*. The remainder of the original submittal formed the basis of the application layer protocol and was placed in this part of ISO 14827. Thus, this part defines only one way to implement the messages that are specified in the format defined by ISO 14827-1. This resulting International Standard supports existing and foreseen data exchange needs using modern design concepts.

Due to the flexibility required by the rapidly developing transport information and control systems (TICS) environment, this part of ISO 14827 uses a very generic structure. Thus, although initially intended to be an International Standard for TICS, it is flexible enough to be used for virtually any data exchange.

ISO 14827-1 explains how to define end-application messages that are to be exchanged between centres for TICS. This definition has been designed to be relatively generic to the selected protocol (e.g. DATEX-ASN, CORBA, etc.) This part of ISO 14827 provides the specification of the Data Exchange protocol in ASN.1 (DATEX-ASN) used to exchange data between central systems. DATEX-ASN was the first protocol standardized because:

- the development of DATEX-Net could be leveraged, and
- there was sufficient market interest to perform the required technical work.

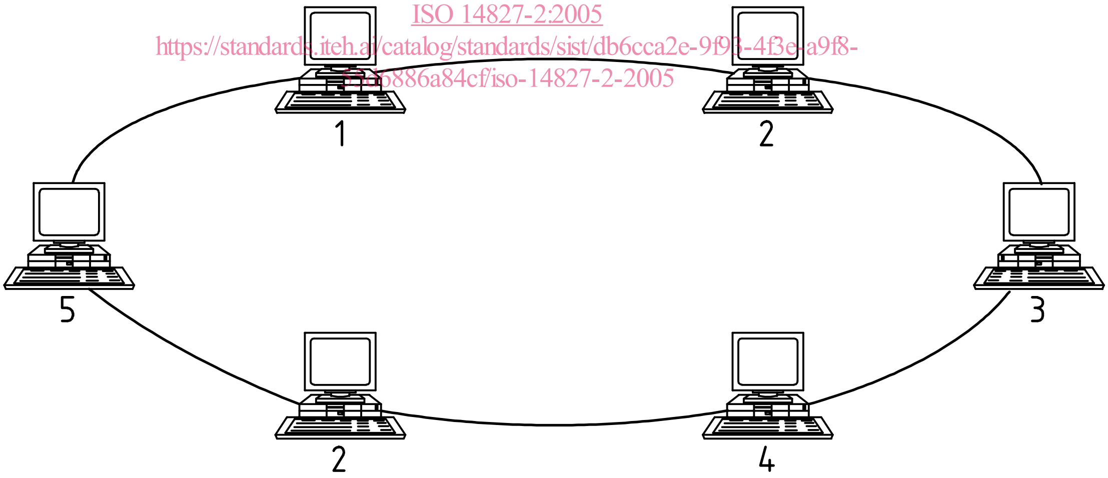
Transport information and control systems — Data interfaces between centres for transport information and control systems —

Part 2: **DATEX-ASN**

1 Scope

DATEX-ASN allows different systems to exchange relevant data. This is contained in end-application messages. Each end-application message is defined as either a “subscription” or a “publication” according to the format as specified in ISO 14827-1. DATEX-ASN defines how these end-application messages are packaged to form a complete data packet and also defines the rules and procedures for exchanging these data packets. Systems using DATEX-ASN are free to implement additional end-application functionalities according to the user requirements.

A DATEX-ASN network comprises a certain number of systems, an example of which is provided in Figure 1.



Key

1 weather system

2 traffic management system

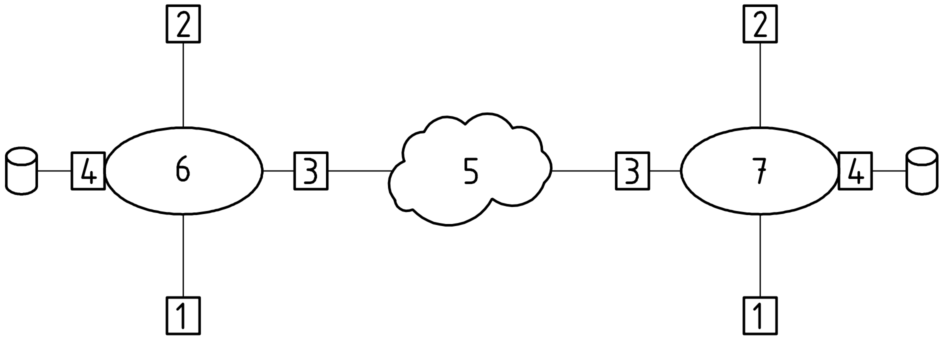
3 transit management system

4 emergency management system

5 information service provider

Figure 1 — An example of a DATEX-ASN network

Each system can be viewed as consisting of the interfaces, as shown in Figure 2:



Key

1 application interface

2 operator interface

3 communication interface

4 database interface

5 communications cloud

6 client system

7 server system

Figure 2 — System interfaces

This part of ISO 14827 deals only with the communications interface. It has been designed to meet the unique requirements of TICS; however, it has been designed in a generic fashion and thus could be used for other data exchanges as well.

Systems implementing this part of 14827 sometimes operate simultaneously as a client and server, using multiple sessions. The communications cloud between the two systems may be complex or simple.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 4217, *Codes for the representation of currencies and funds*

ISO 8824-1, *Information technology — Abstract Syntax Notation One (ASN.1) — Part 1: Specification of basic notation*

ISO 8825-2, *Information technology — ASN.1 encoding rules — Part 2: Specification of Packed Encoding Rules (PER)*

ISO 14827-1, *Transport information and control systems — Data interfaces between centres for transport information and control systems — Part 1: Message definition requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 14827-1 and the following apply.

3.1
connectionless transport profile
service that provides end-system to end-system communications without any connection set-up

EXAMPLE UDP/IP.

3.2
connection-oriented transport profile
service that allows one end-system to exchange a continuous stream of data with another end-system, the data of which is guaranteed to be delivered in the same order in which it was sent without any duplication

NOTE This service is typically achieved by first establishing a connection, then sending the data, and finally terminating the connection.

EXAMPLE TCP/IP.

3.3
data element
syntactically formal representation of some single unit of information of interest (such as a fact, proposition, observation, etc) about some (entity) class of interest (e.g. a person, place, process, property, concept, association, state, event, etc.)

3.4
datagram
entity of data containing enough information to be routed from source to destination without relying on previous network configuration

EXAMPLE IP datagram.

3.5
datagram publication
DATEX-ASN publication (reply) that is sent directly over the given transport profile, in contrast with a file publication

3.6
destination
system or device to which the information in the data packet is intended to be sent

3.7
encoding rules
rules which specify the representation during transfer of the values of ASN.1 types

NOTE 1 Encoding rules also enable the values to be recovered from the representation, given knowledge of the type.

NOTE 2 For the purpose of specifying encoding rules, the various referenced type (and value) notations, which can provide alternative notations for built-in types (and values), are not relevant.

3.8
Ethernet
specific combination of physical and data link layer protocols as defined in IEEE 802.3 that allow multiple systems to gain access to a shared medium and communicate with one another

3.9
file
data storage object, which may be located on any file system such as a hard-disk, a floppy-disk, a RAM-drive, etc.

3.10
file publication
DATEX-ASN publication (reply) that is stored on the server's file system until the client has an opportunity to retrieve it via a file transfer protocol, in contrast with datagram publication

3.11
guaranteed delivery
DATEX-ASN mechanism in which the client acknowledges the receipt of a publication (reply)

3.12
heartbeat
data packet sent to indicate that the sending system is still alive and communicating

3.13
maximum turn-around time
maximum amount of time a system is given to provide an appropriate response to the incoming data packet

3.14
origin
system or device which was the source for all of the information in the data packet

NOTE In many cases, this will be the same as the sender, but could be different. For example, a bridge (or proxy agent) may translate between protocols; in this case the bridge (or proxy agent) would be the sender, while the system generating the data would be the origin.

3.15
port
logical channel in a communications system

NOTE UDP and TCP use port numbers to multiplex data packets from a variety of applications onto a single communications system.

3.16
response time-out period
maximum duration a system is required to wait for a response data packet prior to assuming that the previously sent data packet was never received by the other application

3.17
sender
system which created and sent the DATEX-ASN data packet

3.18
session
period of time during which a client and a server exchange multiple data packets

3.19
silently drop
to ignore a data packet

NOTE A data packet that is silently dropped does not cause any action to occur within the receiving system, nor is any response sent to the subject data packet.

3.20
transport profile
set of services which are responsible for providing a virtually error-free, point-to-point connection so that host A can send data packets to host B and they will arrive uncorrupted

NOTE Connection-oriented transport profiles may also ensure that the data packets arrive in the correct order.

3.21
turn-around time
period of time it takes a client or server to produce and transmit a response data packet, measured starting from the point at which the last byte of data is received from the other system to the point when the last response byte is transmitted

4 Symbols and abbreviated terms

For the purposes of this document, the abbreviated terms of ISO 14827-1 and the following apply.

CMIP	Common Management Information Protocol (RFC 1189)
CORBA	Common Object Request Broker Architecture
D-COM	Distributed Communications Object Model
FDDI	Fibre Distributed Data Interface (ANSI X3T9.5)
FrED	Friendly Exchange of Data
FTP	File Transfer Protocol (RFC 959)
HTML	Hyper Text Mark-up Language (RFC 2854)
HTTP	Hyper Text Transfer Protocol (RFC 2616)
IP	Internet Protocol (RFC 791)
ISDN	Integrated Services Digital Network
NTCIP	National Transportation Communications for Intelligent Transportation Systems (ITS) Protocol
PPP	Point-to-Point Protocol (RFC 1661)
SNMP	Simple Network Management Protocol (RFC 1157)
SQL	Structured Query Language
TCP	Transmission Control Protocol (RFC 793)
TCIP	Transit Communications Interface Profiles
TFTP	Trivial File Transfer Protocol (RFC 1350)
TICS	Transport Information and Control Systems
UDP	User Datagram Protocol (RFC 768)

5 Implementation considerations

Before exchanging data, transportation centres must agree on the specific issues that are described in the list below.

NOTE Some of these issues (e.g. lower layer protocols) may be specified elsewhere. For example, Annex D provides a definition of these traits for standardized IP implementations.

a) General:

1) time period throughout which the overall agreement is valid;

2) rules for terminating the agreement before the expiry time of the agreement;

3) server and client domain names and off-line contact addresses, telephone, fax and e-mail details.

b) Access (DATEX-ASN requires a user-name and associated password.):

1) IP address of the client, assigned by the Internet Assigned Number Authority if the link uses a public network;

2) IP address of the server, assigned by the Internet Assigned Number Authority if the link uses a public network;

3) a list of authorized client user-names, referred to as the user-name used throughout this part of ISO 14827;

4) a password associated with each client user-name.

c) Protocols:

1) selection of lower layer protocols, including:

i) presentation (e.g. BER, EDIFACT, or others) and session layers;

ii) transport and network layers (e.g. UDP/IP, TCP/IP, etc.);

iii) data link and physical layers (e.g. Ethernet, FDDI, PPP over ISDN).

2) maximum datagram size;

3) selection of preferred file transfer protocols.

d) Management of background information:

1) specification of the Data Registry to be used.

e) Message management:

1) messages which must be supported, which may include messages that are standardized in other documents and/or messages unique to the specific implementation.

6 Data exchange procedures

This part of ISO 14827 defines an application layer protocol by which data elements are exchanged between a client and server. Communication between client and server shall be accomplished by the exchange of data packets and files as defined in this section.

6.1 General data packet procedures

DATEX-ASN data packets shall be constructed according to the formally defined ASN.1 data structures defined in Annex A.

6.1.1 Sessions

This part of ISO 14827 requires all data packets to be transmitted in an application session. Within each session, one system shall act as a client and the other shall act as the server.

NOTE Multiple sessions may exist simultaneously. Thus, a pair of systems may have two concurrent sessions, one where System A acts as the client and System B acts as the server and the other where System A acts as the server and System B acts as the client. These sessions would be distinguished by lower layer protocols (e.g. TCP or UDP port numbers).

6.1.2 Transport requirements

Data may be exchanged over connection-less or connection-oriented transport profiles, but a single transport profile shall be used for all data packets exchanged within a session.

EXAMPLE If the first data packet in establishing a session is transmitted using UDP, then all data packets within that session will use UDP. Likewise, if the initial transmission is TCP, then all data packets will be TCP.

6.1.3 Response time-outs

The client and server shall negotiate the response time-out period for each session. The response time-out period should be long enough to accommodate the network propagation delays for both data packets as well as the turn-around time required to handle the message on the receiving end. In theory, this should be measured from when the last byte is transmitted to when the last response byte is received; however, it is expected that most implementations will measure the time from the return from the system write call to the return from the system read call.

NOTE A typical implementation is to set the time-out to be an integral multiple of the turn-around time and the multiplier is typically set to three. However, as some communications media and networks may experience significant delays, the system should allow this multiplier to be set at run-time.

6.1.4 Retransmission

If a specific data packet requires a response and an appropriate response is not received within the response time-out period, the identical data packet (e.g. same data packet number, same time stamp, etc.) shall be retransmitted one time only. If no response is received to the second data packet, prior to a subsequent response time-out period, the data packet transmission shall be considered unsuccessful. If a response is received after the time-out period, it may be ignored.

6.1.5 Duplicate data packets

Any time a client or server receives a data packet that requires a response, a new response data packet shall be prepared and transmitted as soon as possible, even if the received data packet was a duplicate data packet.

6.2 General file procedures

The client may request the publication (reply) data to be sent within the publication data packet, or it may request the publication data to be stored in a file on the server with the publication data packet indicating the file name of the publication file. The file can then be retrieved by the client within the constraints set by the server. Such a publication file shall only contain the "TICS information" as defined by the PublicationData structure as defined in A.9.

6.3 Sessions

Within each session, one system is a client and the other is a server. A server with a given domain name shall not accept more than one session with any client domain name with a given transport profile; however, as a single system may have multiple domain names, multiple sessions could exist between a given client system and server system pair.

NOTE 1 Multiple sessions may exist on a single physical link simultaneously. For example, system A may act as a server in one session with system B while acting as a client in a second session.

NOTE 2 A single client may have sessions with multiple servers simultaneously; thus, the complete session number over any given transport profile is defined by the server domain name followed by the client domain name.

NOTE 3 Some implementations may have a need to frequently publish relatively large data packets. There are various ways to achieve this, including: (1) increasing the UDP/IP datagram size to support the required size; or (2) maintaining a prolonged TCP connection over which the large data packets are periodically sent. The preferred solution will depend on a number of implementation-specific issues such as media quality and required reliability of transmission.

NOTE 4 Simultaneous sessions between a single client and server pair may exist if the sessions use different transport profiles (e.g. one UDP and one TCP).

6.3.1 Establishing a session

The server may wish to establish a session. For example, this may be in order to publish information for a registered subscription (request) or allow a receipt of a subscription if the server is protected by a firewall. In this case, the server shall transmit an “Initiate” data packet, as defined in A.3, with the datex-Destination-txt and datex-Sender-txt fields set to the proper name.

A server should not terminate a session it initiated for a period of one heartbeat duration after final publication.

If the client receives an “Initiate” data packet or if the client wishes to establish a session, the client shall transmit a “Login” data packet, as defined in A.4.

Upon receiving a “Login” data packet, a server shall determine if the domain names, user-name, password, maximum heartbeat duration, response time-out period, allowed encoding rules, datagram size and login reason are valid for the request. The server shall also ensure that a session with the given domain name and transport profile does not already exist. If the request is found to be invalid, the server shall either:

- respond with a “reject” data packet, as defined in A.12, with the “error-code” set to the most appropriate code number which applies to the denial, or
- not respond if the server determines this is appropriate due to security reasons.

If the request is valid, the server shall respond with an “accept” data packet, as defined in A.11, and shall identify the selected encoding rules from the list of options in the login request. This completes the procedures to establish a session.

The procedure to establish a session is summarized in Figure 3. All data packets exchanged during this procedure shall use the encoding rules that were agreed to off-line. All data packets exchanged after the successful completion of this procedure shall use the encoding rules, as negotiated within the “Login” and “Accept” data packets.

EXAMPLE Per Annex D, if the session is established over TCP/IP on Port 355, data packets exchanged during this procedure shall use BER encoding; data packets exchanged after the successful completion of the login process would then use the encoding rules negotiated by the “Login” and “Accept” data packets.

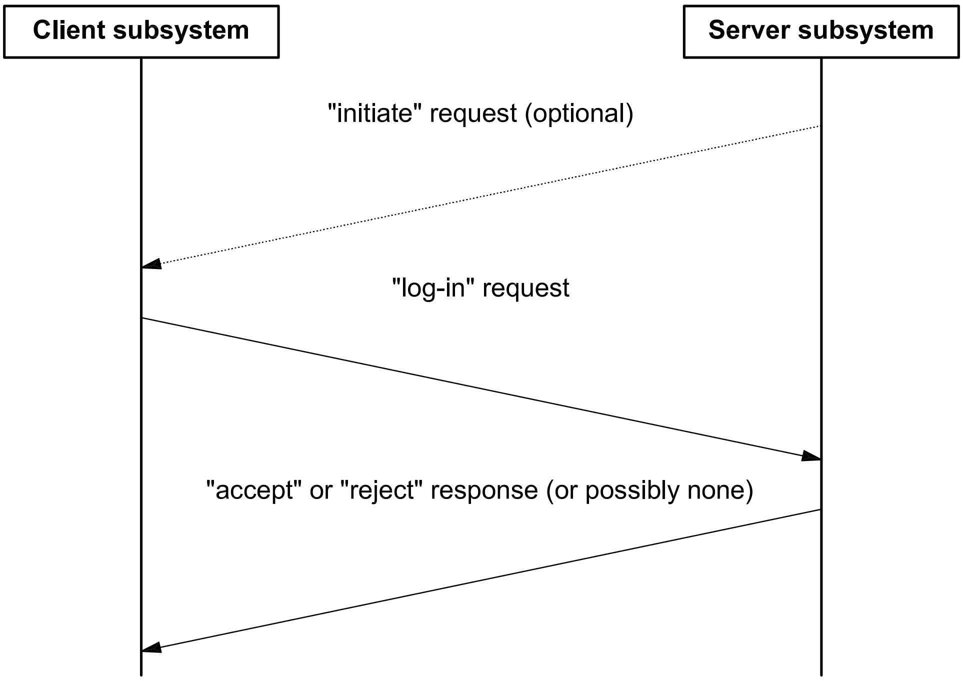

Client subsystem
Server subsystem
"initiate" request (optional)
"log-in" request
"accept" or "reject" response (or possibly none)

Figure 3 — Establishing a session

6.3.2 Maintaining a session

Sessions are maintained by the client and server exchanging “FrED” data packets. If, at any point during a session, no data packets are received from the other system for a period exceeding the maximum heartbeat duration, as specified in the login request, the session shall be immediately terminated by both the client and the server without exchanging any data. This type of termination should only be encountered due to unusual circumstances, e.g. a system crash.

NOTE 1 FrED stands for a “Friendly Exchange of Data”. The data packet is generally used as an acknowledgement data packet, but it is also used as a system heartbeat when there has been a prolonged period of silence. Thus, the term “ack” did not truly apply to this data packet and the committee determined that it should be termed a “FrED”.

NOTE 2 A session may be kept open permanently by meeting the requirements of this subclause.

The client shall maintain the session until the termination procedures are initiated as indicated by 6.3.3. The client shall keep track of the elapsed time since it received a data packet from the server and shall ensure that this time does not exceed the maximum heartbeat duration by generating “FrED” data packets, as defined in A.5, as needed. The DATEX.FrED_ConfirmPacket_number-ulong shall be zero (0) for such “FrED” data packets, hereinafter referred to as “FrED” heartbeat data packets. It is recommended that the client transmit “FrED” heartbeat data packets roughly three times more often than the time specified by the maximum heartbeat duration.

The server shall acknowledge a “FrED” heartbeat data packet by transmitting a “FrED” data packet with the DATEX-FrED_ConfirmPacket_number-ulong set to the packet number of the “FrED” heartbeat data packet which is being acknowledged. This shall complete the session maintenance procedure.

When desired, the session shall be terminated according to the procedure described in 6.3.3.

The procedure to maintain a session is summarized in Figure 4.