BS EN ISO 18750:2018

BSI Standards Publication

Intelligent transport systems - Co-operative ITS - Local dynamic map

Documents
Document Sharing Hub

Full document details: BS EN ISO 18750:2018

National foreword

This British Standard is the UK implementation of EN ISO 18750:2018. It is identical to ISO 18750:2018. It supersedes PD CEN ISO/TS 18750:2015, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Intelligent transport systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 97879 1

ICS 03.220.20; 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2018.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS EN ISO 18750:2018

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 18750

June 2018

ICS 03.220.20; 35.240.60

Supersedes CEN ISO/TS 18750:2015

English Version

Intelligent transport systems - Co-operative ITS - Local dynamic map (ISO 18750:2018)

Systèmes de transport intelligents - Systèmes intelligents de transport coopératifs - État des connaissances des cartes (ISO 18750:2018)

Intelligente Transportsysteme - Kooperative Systeme - Festlegung eines globalen Konzeptes für lokale dynamische Karten (ISO 18750:2018)

This European Standard was approved by CEN on 12 June 2018.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2018 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN ISO 18750:2018 E

Documents
Document Sharing Hub

Full document details: BS EN ISO 18750:2018

European foreword

This document (EN ISO 18750:2018) has been prepared by Technical Committee ISO/TC 204 "Intelligent transport systems" in collaboration with Technical Committee CEN/TC 278 “Intelligent transport systems” the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by December 2018, and conflicting national standards shall be withdrawn at the latest by December 2018.

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

This document supersedes CEN ISO/TS 18750:2015.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 18750:2018 has been approved by CEN as EN ISO 18750:2018 without any modification.

Documents
Document Sharing Hub

Full document details: BS EN ISO 18750:2018

Contents

Page

Foreword ... **v**
Introduction ... **vi**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **2**
4 Symbols and abbreviated terms ... **3**
5 Architectural environment ... **4**
5.1 Local Dynamic Map ... 4
5.2 LDM in an ITS-S ... 4
5.3 LDM in an ITS-SU ... 5
5.4 LDM related processes ... 7
5.4.1 Synchronization of LDMs ... 7
5.4.2 Archiving of LDM Data Objects ... 7
5.5 LDM for road safety and vehicle-to-vehicle applications ... 7
5.6 Security perspective ... 8
5.6.1 Authorised access to LDM ... 8
5.6.2 Initialisation and installation of applications to the BSMD ... 8
5.6.3 Privacy ... 9
5.7 An LDM versus other similar functionalities in an ITS-SU ... 9
6 Functionality ... **9**
6.1 Terms and conventions ... 9
6.2 Structure of an LDM ... 11
6.3 LDM Data Storage ... 12
6.4 LDM services ... 14
6.4.1 Registration, deregistration, and revocation of ITS-S application processes ... 14
6.4.2 Security checking in access requests ... 14
6.4.3 Access request management ... 15
6.5 LDM maintenance ... 17
6.5.1 LDM Area of Maintenance ... 17
6.5.2 Outdated data management ... 17
6.6 LDM knowledge base ... 17
6.6.1 Metadata ... 17
6.6.2 Utility functions ... 18
6.7 Interfaces ... 18
6.7.1 Types of interfaces ... 18
6.7.2 Parameters of interface functions ... 19
6.7.3 LDM application management interface ... 20
6.7.4 LDM data interface ... 22
6.7.5 Security interface ... 25
6.7.6 LDM management interface ... 26
6.7.7 Service access points ... 27
7 Procedures ... **30**
7.1 LDM services ... 30
7.1.1 Registration, deregistration, and revocation of ITS-S application processes ... 30
7.1.2 Security checking in access requests ... 30
7.1.3 Access request management ... 30
7.1.4 Second level filtering ... 32
7.2 LDM maintenance ... 33
7.2.1 Area management ... 33
7.2.2 Outdated data removal ... 33
7.3 LDM knowledge data base ... 33
7.4 Interfaces ... 33

AVA Documents
Document Sharing Hub

© ISO 2018 – All rights reserved

Full document details: BS EN ISO 18750:2018

7.5 LDM management ... 33
7.5.1 Registration of LDM at ITS-S management entity ... 33
7.5.2 Multiple ITS-SCUs ... 33

Annex A (normative) **ASN.1 modules** ... **35**

Annex B (normative) **LDM Data Dictionary** ... **48**

Annex C (informative) **Examples of LDM-DOs** ... **50**

Annex D (informative) **Location-Referencing** ... **57**

Annex E (informative) **Time-Referencing** ... **61**

Annex F (normative) **Implementation Conformance Statement proforma** ... **62**

Bibliography ... **68**

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/TC 204, *Intelligent transport systems*.

This first edition cancels and replaces the first edition (ISO/TS 18750:2015), which has been technically revised.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

Introduction

An essential property of cooperative intelligent transport systems (C-ITS), see ISO TR 17465-1[17], is the sharing of data between different ITS applications providing different ITS services to the users. This approach replaces the traditional approach where each application is operated in an isolated environment, i.e. referred to as "silo - approach". The C-ITS approach enables synergies in components of an ITS station unit, e.g. sharing of communication tools, improves overall performance and reliability, and reduces overall cost. In order to protect the interests of the various ITS applications, C-ITS implements the concept of an ITS station operated as a bounded secured managed domain.

The sharing of data between applications is achieved by subscribe/publish mechanisms, where at least two mechanisms are distinguished, i.e. one allowing ITS-S application processes to subscribe to standardized messages from ITS message sets (direct forwarding upon reception of such messages in an ITS station unit), and one using a local dynamic map (LDM) as repository of standardized data objects. Such data objects stored in an LDM are named LDM Data Objects (LDM-DOs). LDM-DOs provide self-consistent information on real objects existing at a given geo-location during a given lifetime-interval. Authorized ITS-S application processes may add LDM-DOs to an LDM, and may retrieve LDM-DOs from an LDM. Retrieval of LDM-DOs may be performed in queries and by means of subscription. A subscription will result in automatic notifications of selected LDM Data Objects either in defined time intervals, or event driven.

This document introduces the usage of LDMs, and specifies the LDM for global usage in C-ITS.

Initial implementations of LDMs were in the EU research projects CVIS[40] and Safespot[42].

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

Intelligent transport systems — Co-operative ITS — Local dynamic map

1 Scope

This document:

— describes the functionality of a "Local Dynamic Map" (LDM) in the context of the "Bounded Secured Managed Domain" (BSMD);

— specifies:

  — general characteristics of LDM Data Objects (LDM-DOs) that may be stored in an LDM, i.e. information on real objects such as vehicles, road works sections, slow traffic sections, special weather condition sections, etc. which are as a minimum requirement location-referenced and time-referenced;

  — service access point functions providing interfaces in an ITS station (ITS-S) to access an LDM for:

    — secure add, update and delete access for ITS-S application processes;

    — secure read access (query) for ITS-S application processes;

    — secure notifications (upon subscription) to ITS-S application processes;

    — management access:

      — secure registration, de-registration and revocation of ITS-S application processes at LDM;

      — secure subscription and cancellation of subscriptions of ITS-S application processes;

  — procedures in an LDM considering:

    — means to maintain the content and integrity of the data store;

  — mechanisms supporting several LDMs in a single ITS station unit.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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/IEC 8824-1, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation*

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

ISO/IEC 9646-7, *Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 7: Implementation Conformance Statements*

ISO 21217, *Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture*

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1
data integrity
property that data has not altered or destroyed in an unauthorized manner

[SOURCE: ISO 24534-5]

3.2
International Atomic Time
time since 00:00:00 UTC, 1 January, 2004, identical with UTC except that no leap seconds need to be added

3.3
LDM Area of Interest
location requirement used in the filter process of queries and automatic notifications

3.4
LDM Area of Maintenance
information on the operational location area of an LDM used by LDM maintenance

Note 1 to entry: ETSI EN 302 895[30] restricts the LDM Area of Maintenance to "geographical area specified by the LDM for LDM maintenance".

3.5
LDM Permissions
information on how a specific ITS-S application process may use an LDM

3.6
LDM Data Object
location-referenced and time-referenced representation of a real object that is self-explanatory without any further context information

3.7
LDM Data Object ID
identifier of an LDM Data Object which is unique in an LDM

3.8
LDM Data Dictionary
dictionary of LDM Data Object Types

3.9
LDM Data Object Type
identifier of the type of information contained in an LDM Data Record

3.10
Location Validity
information indicating a location at which an LDM Data Object is valid

3.11
Time Validity
information indicating a time interval during which an LDM Data Object is valid

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

3.12
LDM Time of Interest
time requirement used in the filter process of queries and automatic notifications

3.13
Local Dynamic Map
entity consisting of LDM Data Objects, services and interfaces for manipulating these LDM Data Objects

3.14
location reference
uniquely identifiable description of position or area in the real world

3.15
metadata
data about data

Note 1 to entry: The term "metadata" is ambiguous as it is used for fundamentally different concepts. Structural metadata is information related to the design and specification of data structures; it is also referred to as "data about the containers of data". Descriptive metadata is information on instances of data, i.e. the data content; it is also referred to as "data about data content".

3.16
Time of Creation
time when an LDM Data Record was created and updated

3.17
Time of Deletion
time when an LDM Data Record may be deleted and will no longer be considered by the LDM search functionality

3.18
Time of Generation
time when the content of the LDM Data Object information field was created

Note 1 to entry: This is different to the time, when the LDM Data Object was written into an LDM.

4 Symbols and abbreviated terms

BSMD	Bounded Secured Managed Domain
BSME	Bounded Secured Managed Entity
IAT	International Atomic Time
ICS	Implementation Conformance Statement
ITS	Intelligent Transport Systems
ITS-SCU	ITS Station Communication Unit
ITS-SU	ITS Station Unit
IUT	Implementation Under Test
LDM	Local Dynamic Map
LDM-DD	LDM Data Dictionary
LDM-DT	LDM Data Type

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

LDM-DAT	LDM Data Attribute Type
LDM-DATID	LDM-DAT Identifier
LDM-DTID	LDM-DT Identifier
NoO	Notification of Obligations
OoT	Obligation of Trust
PMI	Privilege Management Infrastructure
SAO	Signed Acceptance of Obligations
SUT	System Under Test
TPEG	Transport Protocol Experts Group
UTC	Universal Time Coordinated

5 Architectural environment

This clause contains informative descriptions of the architectural environment of an LDM.

5.1 Local Dynamic Map

A Local Dynamic Map (LDM) is an entity consisting of LDM Data Objects, services and interfaces for manipulating these LDM Data Objects (LDM-DO). LDM-DOs are distinguished by means of their LDM Data object Type (LDM-DT). LDM-DTs are specified by registration in an LDM Data Dictionary (LDM-DD). The concept of the LDM-DD is specified in Annex B.

NOTE In ISO TR 17424[18], LDM-DOs are classified into Type 1 (static permanent data objects, e.g. cartographic data),[2] Type 2 (static transitory data objects, e.g. temporary parking lot on the road), Type 3 (dynamic transitory data objects, e.g. works location), and Type 4 (highly dynamic data objects, e.g. location, orientation and speed of surrounding vehicles). This classification is not used in this document.

An LDM-DO provides information on real objects (cars, road events, ...) that exist at a defined location, e.g. in a defined geo-area, and within a defined time interval. In the uppermost simple case the information provided by an LDM-DO is just its type, its geo-location, and its time interval of validity. Such information may be received in an ITS station unit via different channels such as:

— DATEX II[34], TPEG[38], RDS-TMC (legacy systems);

— CEN / ETSI / ISO / SAE ITS Message sets EN/ISO 19091[19], ISO/TS 19321[20], ETSI EN 302 637-2[28], ETSI EN 302 637-3[29], SAE J2735[39];

composed of different sets of attributes, and presented in different formats (encodings). ITS-S application processes capable to receive this information perform a mapping on LDM-DOs and a translation of attribute formats into the common format given by the LDM-DTs.

5.2 LDM in an ITS-S

The local dynamic map (LDM) specification provided in this document is designed for the architectural environment of an ITS station operated as a Bounded Secured Managed Domain (BSMD) specified in ISO 21217 and illustrated in Figure 1.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

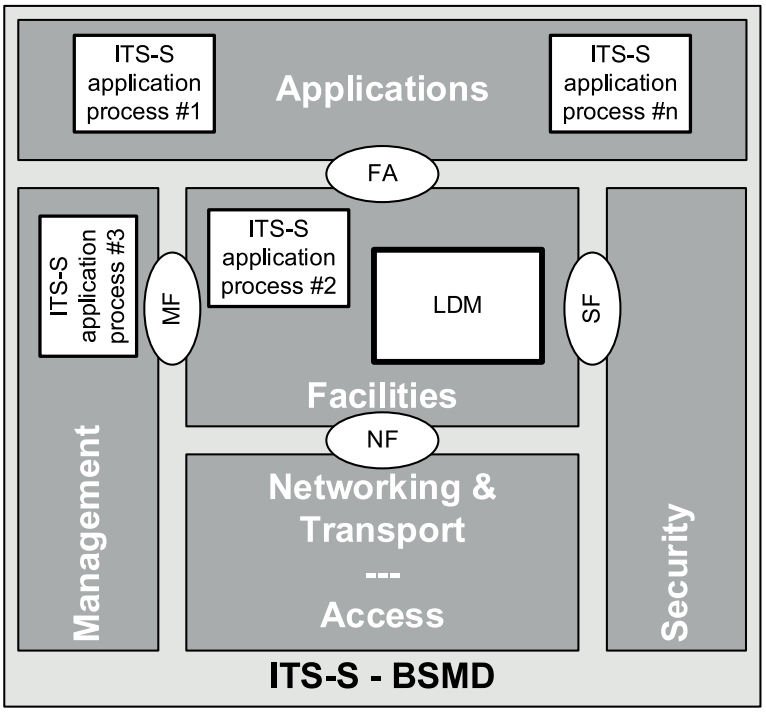

Figure 1 — LDM in an ITS-S operated as a Bounded Secured Managed Domain (BSMD)

The LDM functionality specified in Clause 6 is located in the ITS-S facilities layer. An LDM interfaces with ITS-S application processes specified in ISO 21217. The interface functionality is specified in 6.6.2 by means of functions of services of the FA-SAP and the MF-SAP; both Service Access Points (SAPs) offer identical functions for this purpose. The generic services of FA-SAP and MF-SAP are specified in ISO 24102-3[11].

5.3 LDM in an ITS-SU

Various examples of supported implementation configurations are illustrated in Figure 2, Figure 3, Figure 4, and Figure 5.

Figure 2 illustrates a "single-box" configuration of an ITS station unit (ITS-SU) with a single LDM.

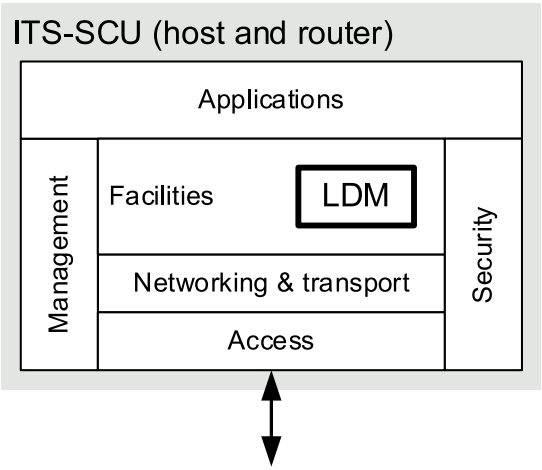

Figure 2 — Implementation configuration example a)

Figure 3 illustrates a "single-box" configuration of an ITS-SU with two LDMs.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

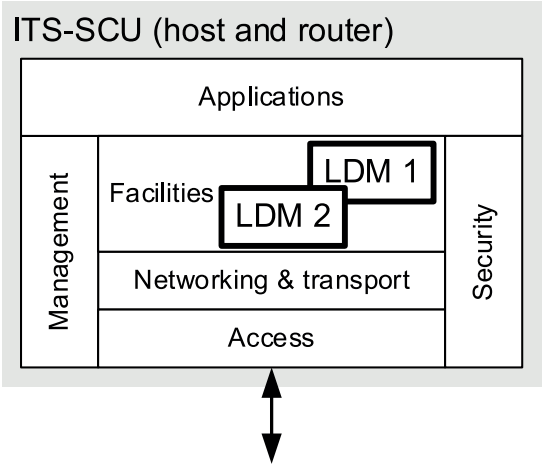

Figure 3 — Implementation configuration example b)

Figure 4 illustrates a configuration of an ITS-SU with two ITS station communication units (ITS-SCU). One of these ITS-SCUs has a host-only role specified in ISO 21217 and contains a single LDM. The other ITS-SCU has a router-only role specified in ISO 21217 and does not contain an LDM.

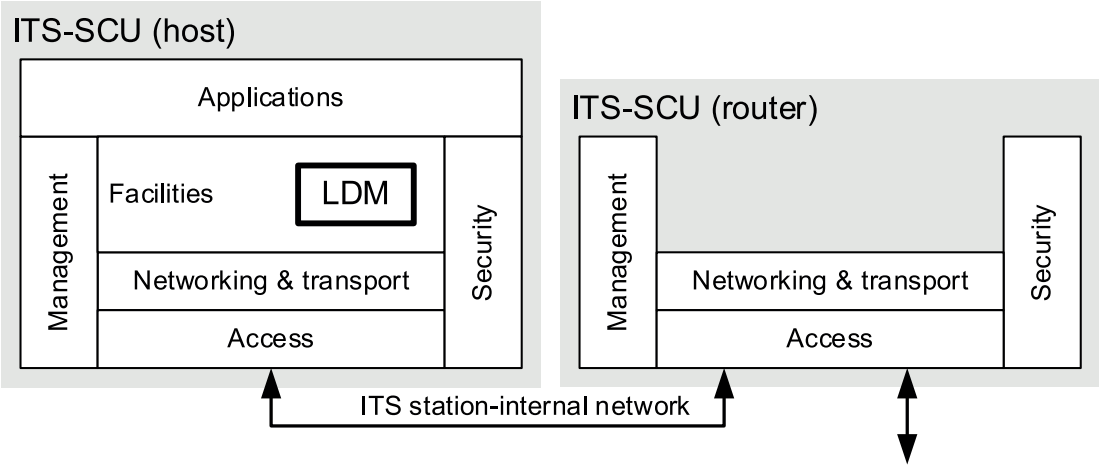

Figure 4 — Implementation configuration example c)

Figure 5 illustrates a configuration of an ITS-SU with two ITS station communication units (ITS-SCU). One of these ITS-SCUs has a host-only role specified in ISO 21217 and contains a single LDM. The other ITS-SCU has a host-and-router role specified in ISO 21217 and contains also an LDM.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

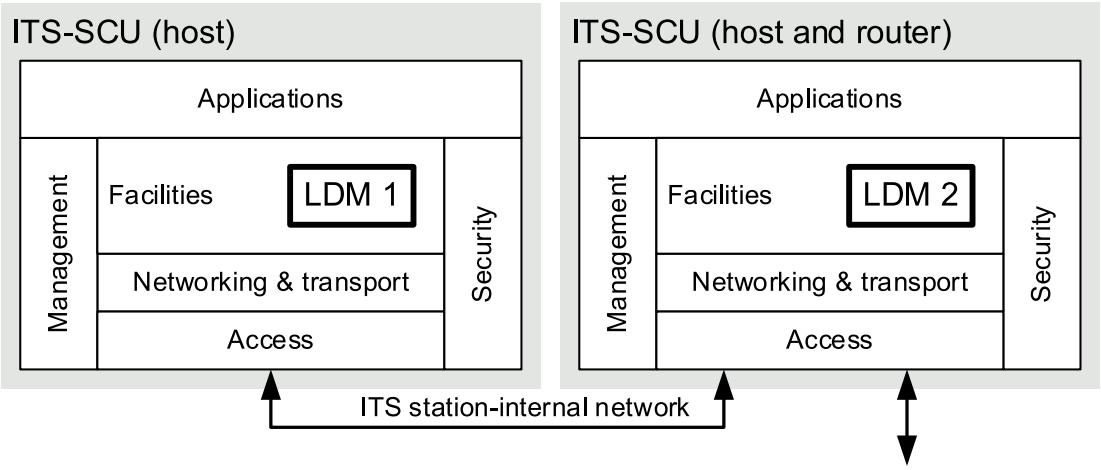

Figure 5 — Implementation configuration example d)

Many other implementation configurations are feasible.

NOTE In ITS-SUs composed of several ITS-SCUs the ITS station management can use the "ITS station-internal management communications protocol" (IICP) specified in ISO 24102-4[12] to support overall station management.

5.4 LDM related processes

5.4.1 Synchronization of LDMs

The concept of synchronization of LDMs is introduced in ISO TR 17424[18], distinguishing:

— synchronization of LDMs operated in ITS station units of different vehicles;

— synchronization of LDMs operated in ITS station units at the roadside, in central offices and in vehicles.

Reference is made to means which are already in use for TPEG and DATEX.

Such synchronization means updating of an LDM by an authorized "master" LDM. As only ITS-S application processes can access LDM-DOs, any synchronization is to be realized by ITS applications. Details are outside the scope of this document.

NOTE Updates of information in an ITS-SU can be performed using remote management standardized in ISO 24102-2[10].

5.4.2 Archiving of LDM Data Objects

Archiving of LDM Data Objects is a feature that produces a kind of log-file of an LDM. Such log-file information might be of interest for different purposes, but might also be subject to privacy considerations.

This document specifies neither an archiving functionality nor related interfaces. Archiving can be implemented in a non-standardized way.

5.5 LDM for road safety and vehicle-to-vehicle applications

An LDM dedicated to usage for road safety and vehicle-to-vehicle applications (electronic horizon) is specified by ETSI in EN 302 895[30]. This ETSI LDM specification constitutes a functional sub-set of the specification provided in this document.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

5.6 Security perspective

5.6.1 Authorised access to LDM

The architecture of an LDM in the context of BSMD from a security perspective is to ensure that access is restricted to identified and authorised ITS-S application processes. Application processes not certified for operation in a BSMD may access an LDM via a secure gateway described in ISO 21217, where the firewall ITS-S application process of this gateway is authorised for read-access to the LDM.

All the core assets are to be considered as vulnerable and therefore subject to protection, where protection takes the form of specific guards. The guard mechanism used in protecting the LDM is a policy based access control scheme where ITS-S application processes will pre-register their policy with the ITS-S and if that policy is agreed all future access by the ITS-S application process will be verified as being consistent with the policy.

5.6.2 Initialisation and installation of applications to the BSMD

The kernel of an ITS-SCU forms a trust centre of the BSME and is identifiable to third party ITS-S application processes as such. Any ITS-S application process to be added to an ITS-SCU within the BSME verifies the identity and capability of the ITS-SCU prior to installation. If installation is allowed an ITS-SCU verifies the credentials offered by the ITS-S application process. Prior to distribution each ITS-S application process is functionally verified and tested and assertions of required functionality, of developer identity, and of the tester, are validated prior to installation ISO 17419[21].

The core model follows that developed in the i-Tour project[41] as an extension of an "Obligation of Trust" (OoT) protocol, extending the models used for Java midlet distribution used in many common application stores, see ISO 17419[21]. The protection framework is a form of a Privilege Management Infrastructure (PMI) based on common cryptographic modules and processing where authorisation is viewed as a set of mutually agreed actions through the assignment of permissions to the parties, i.e. the LDM and the LDM user. In the OoT protocol the participating parties exchange difficult-to-repudiate digitally signed obligating constraints, also referred to as "Notification of Obligations" (NoO), which detail their requirements for sending their sensitive information to the other party, and proof of acceptances, also referred to as "Signed Acceptance of Obligations" (SAO), which acknowledge the conditions they have accepted for receiving the other party's sensitive information. The required capabilities of the LDM user, i.e. an ITS-S application process, to be installed will be declared and the application restricted to use only those capabilities by means of a policy enforcement engine acting in the role of a Policy Enforcement Point in the LDM itself.

For protection of data the data objects identified below capture the primary policy elements PrivacyPolicyDirective, SecurityPolicyDirective, SignedPrivacyPolicy, SignedSecurityPolicy, CounterSignedPrivacyPolicy, and CounterSignedSecurityPolicy.

The privacy policy directive is a set of policy statements that identify the identity of the data controller. The privacy enforcement point agrees to implement the policy and to indicate that in the Signed Privacy Policy where the signature is of the data processor (acting as policy enforcement point).

Acceptance of the privacy policy is notified by the client in the Countersigned Privacy Policy where the signature is given by the client using the pseudonymous identity agreed during registration. The retention of the countersigned policy agreement provides the basis of non-repudiation of consent.

NOTE The data privacy legislation in Europe assumes the presence of a number of entities in a system dealing with private data. These are the data controller, data processor and data subject, and a contract of consent. In an all informed C-ITS there is no a priori consent establishment between the transmitting ITS-SU and any of the receiving ITS-SUs, thus the security model attempts to minimize the possibility of any personal data being made known to a receiving ITS-SU. The model therefore virtualizes the functionality of data controller, data processor and consent by use of verifiable proofs of authority to act on data.

Permissions resulting from policy are of type "Permit" and "Deny" based on authorization, i.e. after application of the policy the request is either permitted or denied. Requests themselves may contain specific access requests, e.g. read data from the LDM, write data to the LDM.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

Every incoming command to the LDM is associated with a set of claims that are checked against the local policy at the PEP in the LDM. If any data access attempt from an application is made post-registration and post-acceptance of the policy that does not comply with the policy it is denied.

5.6.3 Privacy

The C-ITS enforces pseudonymity capabilities through the security functions described, e.g. in ETSI TS 102 940[32] and ETSI TS 102 941[33] which maintains privacy control of data entered into the LDM.

5.7 An LDM versus other similar functionalities in an ITS-SU

The sharing of data between ITS-S application processes in an ITS-SU can be achieved by subscribe/publish mechanisms, where at least two mechanisms are distinguished, i.e.

a) one allowing ITS-S application processes to subscribe at the ITS-S facilities layer to standardized messages from ITS message sets as specified in ISO/TS 17429[22] without using an LDM, and

b) one using a local dynamic map (LDM) as repository of standardized data objects.

The approach a) specified in ISO/TS 17429[22] standardizes an ITS-S facility layer message handler which can

— directly forward complete received messages to subscribed ITS-S application processes without storing these messages, and

— present LDM Data Objects to an LDM in case these LDM Data Objects are contained in messages that follow the message format convention of this message handler.

There may be also other data storages, which are basically different to an LDM, i.e. which may store data objects that are not following the definition of an LDM-DO.

6 Functionality

This clause contains informative descriptions of the functionality of an LDM.

6.1 Terms and conventions

As explained in 5.1, an LDM deals with information on real objects that are existent at a defined location (geo-area) and within a defined time interval. Such information on a real object is identified in an **LDM Data Record**, see Figure 7. Every LDM Data Record is identified with a unique LDM Data Record ID; the value zero indicates an "unknown record".

Different location and time definitions are used to define the functionality of an LDM.

— Definitions related to the information on the real object

  — **Location Validity**

    Information at which geo-location or in which geo-area the LDM-DO applies.

  — **Time Validity**

    Information in which time interval(s) the LDM-DO applies.

  — **Time of Generation**

    Information on the time when the LDM-DO information was generated, e.g. time when a perception system (e.g. a sensor) detected the event "slippery road".

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

- **Time of Mandatory Deletion**

  Information on time after which the LDM record will no longer be returned in a query.

- Definitions used in queries
  - **LDM Area of Interest**

    Geo-location(s) or geo-area(s) that are of interest for the querying ITS-S application process.

  - **LDM Time of Interest**

    Time instant or time interval(s) that are of interest for the querying ITS-S application process.

  - **Age of Interest**

    Age of LDM record as required by the querying ITS-S application process. The age is calculated with a numerical operator presented by the ITS-S application process against the time of generation of an LDM-DO, if available, or alternatively against the time of last update of an LDM-DO.

- Definitions used for maintenance purposes
  - **LDM Area of Maintenance**

    Geo-area(s) considered by the LDM search functionality and defined by the LDM in an implementation-specific way. Without overlap of the LDM Area of Interest with the LDM Area of Maintenance a query will not result in a hit. Note that the area of maintenance can be defined relative to the momentary location of the host ITS-S.

  - **LDM Inactive Area**

    Geo-area(s) considered by the LDM to store LDM records with are not considered by the search functionality; there is no overlap between the LDM Area of Maintenance and the LDM Inactive Area. Details on the usage of the LDM Inactive Area are not specified in this document.

  - **Time of Creation**

    Time at which the LDM record was created in the LDM Data Storage.

  - **Time of Deletion**

    Time after which an LDM record may be deleted, and will no more be considered by the LDM search functionality.

Several location reference systems and time reference systems are known; examples are presented in Annex D and Annex E. This document supports any kind of reference system by defining time reference and location reference with the ASN.1 type CLASS which allows defining specific instantiations at a later time according to the needs of C-ITS services. The generic approach for location is given in the ASN.1 type `LDMarea`. The generic approach for time is given in the ASN.1 type `TimeInformation`.

In order to manage time an LDM needs to maintain or access a time reference system (clock). This document assumes that there is a trusted time service available in an ITS-SU which can be used in an implementation specific way. Time synchronization with an external clock to ensure unique time information in all ITS-SUs will be a task of the ITS-S management of an ITS-S facility, e.g. as specified in ISO 21176[23].

Similarly it is assumed that an LDM has access to a service providing continuously the kinematic state of the ITS-SU in which it resides; thus no explicit interface to such a service is specified in this document.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

As this document supports various implementation architectures illustrated in 5.3, ITS-S application processes need to be enabled to select appropriate LDMs. For this purpose,

a) LDMs are identified by an LDM ID that is unique in an ITS-SU,

b) LDMs register at the ITS-S management entity reporting about their capabilities in terms of supported LDM-DOs, and

c) ITS-S application processes register at the ITS-S management entity reporting their LDM requirements in terms of required LDM-DOs, which is acknowledged by providing the address information of the best suited LDMs.

The LDM performs the following procedures to maintain integrity of the LDM Data Storage:

— Removal of LDM Data Records that are out of date;

— Removal of LDM Data Records which are out of the LDM Area of Maintenance.

Further integrity checking is supposed to be performed by ITS-S application processes.

6.2 Structure of an LDM

An LDM is composed of functional blocks presented in Figure 6:

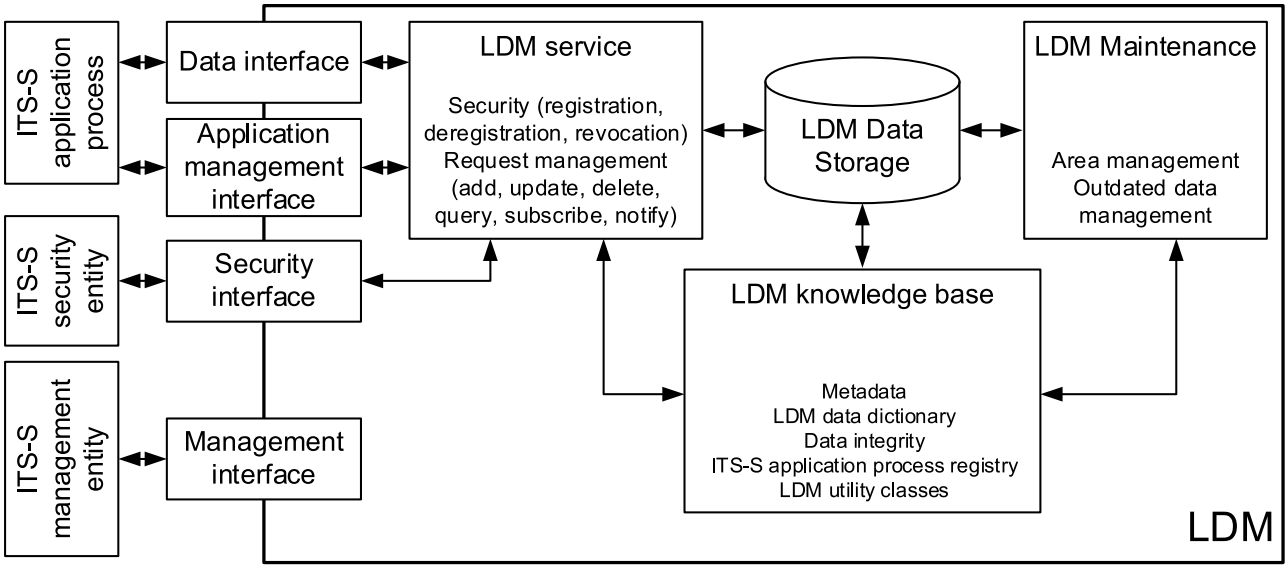

Figure 6 — Structure of an LDM

— **LDM Data Storage**: This is the entity in an LDM that stores LDM-DOs as described in 6.3.

— **LDM Service**: This functional block provides means for:

  — managing registration, deregistration requests and revocation of ITS-S application processes;

  — security checking in access requests;

  — managing access requests (add, update, delete, subscribe, query, notify) from ITS-S application processes;

  as described in 6.4.

— **LDM Maintenance**: This functional block provides means for:

  — updating the LDM Area of Maintenance;

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

— removing LDM-Data Records;

as described in 6.5.

— **LDM Knowledge Base**: This provides the knowledge that is required in the LDM for internal processing as described in 6.6. This functional block includes:

— Metadata;

— the LDM Data Dictionary;

— information on ITS-S application processes' registrations and subscriptions to the LDM;

— LDM utility functions.

— **Interfaces**: The interfaces used and offered by an LDM are:

— Data interface towards ITS-S application processes for:

— add, update and delete access;

— query access;

— subscription access;

— notifications upon subscription.

— Management and security interfaces for:

— registration, deregistration and revocation of ITS-S applications;

— validation of access rights claimed by ITS-S applications at time of registration;

— LDM management (e.g. registration of LDM at the ITS-S management);

as described in 6.6.2.

— **LDM Management**: This functional block provides means for:

— registration of an LDM at the ITS-S management.

6.3 LDM Data Storage

An LDM Data Storage logically contains LDM data records presented in Figure 7.

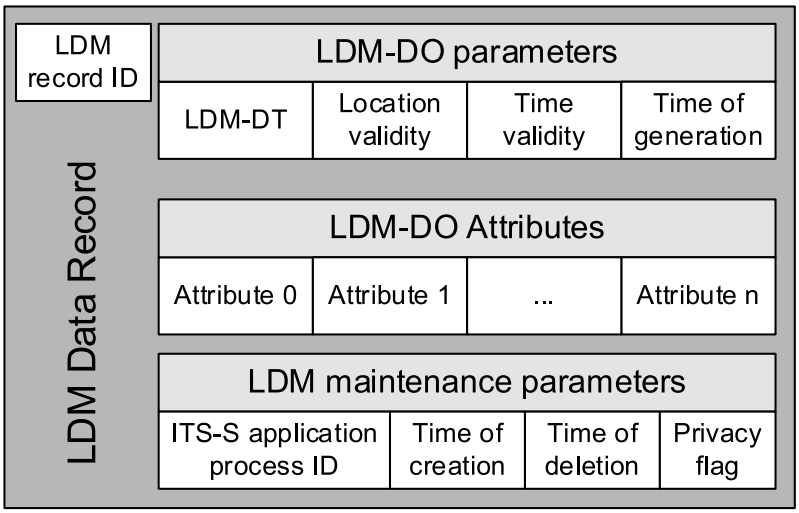

Figure 7 — Elements of LDM Data Record

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

An LDM data record is uniquely identified by its LDM record ID. An LDM data record consists of:

— **LDM-DO Parameters**:

  — the LDM-DO Type (LDM-DT);

  — the Location Validity of the real object;

  — the Time Validity of the real object;

  — Time of Generation of information contained in the LDM-DO (set to the value zero in case the time is unknown);

  — Time of Mandatory Deletion of an LDM Data Record;

  NOTE 1 Updates of an LDM Data Record can only be provided by the same ITS-S application process that originally generated the LDM Data Record.

  NOTE 2 The Location Validity and Time Validity fields basically consist each of two parts, one containing the values of the original reference system, and the other one containing the values of the reference system used in the LDM.

— the **LDM-DO Attributes** as specified in the LDM Data Dictionary (LDM-DD);

— **LDM Maintenance Parameters** which cannot be set explicitly by an ITS-S application process, and which cannot be retrieved by an ITS-S application process:

  — identifier of the ITS-S application process that presented this instantiation of an LDM-DO for storing in the LDM;

  — Time of Creation of the LDM Data Record which is different to the time of generation of the information contained in the attributes of the LDM-DO;

  — Time of Deletion of the LDM Data Record from the LDM;

  — Privacy flag.

Table 1 explains and specifies the elements of an LDM Data Record in Figure 7; it refers to ASN.1 type definition specified in Annex A.

Table 1 — LDM Data Record elements

Element	Specification and explanation
LDM record ID	This element uniquely identifies a specific record in the LDM. The format of this element is given by the ASN.1 element `LDMrecordID` specified in Annex A. The value zero points to the "non-existent" LDM Data Record.
LDM-DO type	This element uniquely identifies the type of the LDM-DO. The format of this element is given by the ASN.1 element `LDMdataObjectTypeID` specified in Annex A.
Location Validity	This element uniquely identifies the position or area at which the information given by the LDM-DO applies. Several location reference systems are allowed in the interface functions. This field basically consist of two parts, one containing the values of the original reference system, and the other one containing the values of the reference system used in the LDM. The format of location reference systems is given by the ASN.1 element `LDMarea` specified in Annex A.
Time Validity	This element uniquely identifies the time period when the information given by the LDM-DO applies. Several time formats to present a time period are allowed in the interface functions. Thus this field basically consist of two parts, one containing the values of the original reference system, and the other one containing the values of the reference system used in the LDM. The format of time reference systems is given by the ASN.1 element `TimeInformation` specified in Annex A.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

Table 1 *(continued)*

Element	Specification and explanation
Time of Generation	This element uniquely identifies the time when the data contained in the LDM-DO was generated. Note that this is different to the time of creation when the LDM Data Record was stored in the LDM. The format of this element is given by the ASN.1 element `TimeOfGeneration` specified in Annex A.
Time of Mandatory Deletion	This element is used to indicate up to which time the LDM Data Record may be maintained in the LDM. After this time, the LDM Data Record has to be removed from the LDM. This allows ITS-S applications to request timely deletion of LDM Data Records due to e.g. privacy regulations or privacy policies. The format of this element is given by the ASN.1 element `TimeOfDeletion` specified in Annex A.
LDM Data Object	This element is an instance of the LDM-DT as specified in the LDM-DD. The format of this element is given by the ASN.1 element `LDMdataObject` specified in Annex A.
ITS-S application process ID	This is the identifier of the instance of the the ITS-S application process specified in Table 2 that presented the LDM-DO to the LDM. The format of this element is given by the ASN.1 element `ITSsapiid` specified in Annex A.
Time of Creation	This element identifies two time events, i.e. the time when the LDM Data Record was added to the LDM, and the time when an existing record was updated. The format of this element is given by the ASN.1 element `TimeOfCreation` specified in Annex A.
Time of Deletion	Time of Deletion of an LDM Data Record from an LDM is identical with Time of Mandatory Deletion - if set by an ITS-S application process - or may be derived from the element Time Validity. This time information indicates the time from which on the LDM Data Record will no more be disclosed to ITS-S application processes, and may be archived and deleted from the data store. In case Time of Mandatory Deletion is set archiving is prohibited. The format of this element is given by the ASN.1 element `TimeOfDeletion` specified in Annex A.
Privacy flag	This element is a Boolean flag indicating with the true-value that the LDM Data Record has to be deleted once Time of Deletion passed. The privacy flag may be set by different means. In case Time of Mandatory Deletion is presented with a valid value, the privacy flag is set to true. Default value is false. The format of this element is given by the ASN.1 element `PrivacyFlag` specified in Annex A.

6.4 LDM services

6.4.1 Registration, deregistration, and revocation of ITS-S application processes

An ITS-S application process, see 5.6, presents security credentials including a list of permissions at time of registration at an LDM. An LDM uses services of the ITS-S security entity to check the validity of claimed permissions through the registration and verification of the access control policy for the application.

Security services in the ITS-S security entity continuously check whether an authorization of an ITS-S application process needs to be revoked completely or in parts.

An ITS-S application process may also deregister from an LDM, which disables subsequent attempts to use the LDM.

A normative specification of the related procedure is presented in 7.1.1.

6.4.2 Security checking in access requests

Every access request to the LDM, see 6.4.3, is associated with a set of claims that are checked against the local policy at the PEP in the LDM. If any data access attempt from an application is made post-registration and post-acceptance of the policy that does not comply with the policy it is denied.

A normative specification of the related procedure is presented in 7.1.2.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

6.4.3 Access request management

6.4.3.1 Overview

Request management includes:

— add an LDM Data Record as described in 6.4.3.2;

— update an LDM Data Record as described in 6.4.3.3;

— delete an LDM Data Record as described in 6.4.3.4;

— query LDM-DOs as described in 6.4.3.5;

— subscribe and unsubscribe for updates of LDM-DOs as described in 6.4.3.6;

— notify updates of LDM-DOs as described in 6.4.3.8.

As part of the request management filtering is applied in queries and in subscriptions. ITS-S application processes present the properties upon which queries and subscriptions are performed. First level filtering uses the following parameters presented in Figure 7:

— LDM-DO ID, record ID;

— LDM-DT;

— LDM Area of Interest, e.g. absolute area or area relative to position and movement of ITS-SU;

— LDM Time of Interest;

— Age of Interest;

— any combination of the above listed properties applying simultaneously (logical AND).

A second level filter process selects those pre-filtered LDM-DOs with attribute values that meet requested conditions as described in 6.4.3.9.

NOTE For some applications, e.g. crash avoidance, it is necessary to track the movement of a real object. Such trajectories can be produced by ITS-S application processes based on LDM-DOs related to this real object.

6.4.3.2 Add LDM data record

Upon successful registration at an LDM, see 6.4.1, an ITS-S application process may request adding an LDM data record to the LDM using the interface function of ASN.1 type `LDMaddRequest` specified in 6.7.4.1. In case the ITS-S application process is permitted to add an LDM-DO of a specific LDM-DT, the request is granted and the LDM Data Record is created. This request is acknowledged with the interface function of ASN.1 type `LDMaddConfirm` specified in 6.7.4.1, returning the LDM record identifier of ASN.1 type `LDMrecordID`.

A normative specification of the related procedure is presented in 7.1.3.1.

6.4.3.3 Update LDM data record

An ITS-S application process that successfully requested adding an LDM data record to the LDM, see 6.4.3.2, may subsequently update the LDM data record identified by the LDM record identifier using the interface function of ASN.1 type `LDMupdateRequest` specified in 6.7.4.2. This request is acknowledged with the interface function of ASN.1 type `LDMupdateConfirm` specified in 6.7.4.2.

A normative specification of the related procedure is presented in 7.1.3.3.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018

6.4.3.4 Delete LDM data record

An ITS-S application process that successfully requested adding an LDM data record to the LDM, see 6.4.3.2, may subsequently delete the LDM data record identified by the LDM record identifier using the interface function of ASN.1 type `LDMdeleteRequest` specified in 6.7.4.3. This request is acknowledged with the interface function of ASN.1 type `LDMdeleteConfirm` specified in 6.7.4.3.

A normative specification of the related procedure is presented in 7.1.3.4.

6.4.3.5 Query LDM-DO

Upon successful registration at an LDM, see 6.4.1, an ITS-S application process may request retrieval of LDM-DOs from the LDM using the interface function of ASN.1 type `LDMqueryRequest` specified in 6.7.4.6. In case the ITS-S application process is permitted to query LDM-DOs of the specific LDM-DT, the request is granted and LDM-DOs of the requested LDM-DT are retrieved with the interface function of ASN.1 type `LDMqueryConfirm` specified in 6.7.4.6 considering the filter parameters presented in the request.

A normative specification of the related procedure is presented in 7.1.3.5.

6.4.3.6 Subscribe for updates of LDM-DOs

Upon successful registration at an LDM, see 6.4.1, an ITS-S application process may request subscription to updates of LDM-DOs from the LDM using the interface function of ASN.1 type `LDMsubscribeRequest` specified in 6.7.4.5. In case the ITS-S application process is permitted to subscribe to automatic notifications of updates of LDM-DOs of the specific LDM-DT, the request is granted and acknowledged with the interface function of ASN.1 type `LDMsubscribeConfirm` specified in 6.7.4.5. Upon updates of LDM-DOs subject to a subscription, these updates will be notified automatically to the ITS-S application process.

A normative specification of the related procedure is presented in 7.1.3.6.

6.4.3.7 Unsubscribe for updates of LDM-DOs

Upon successful subscription for updates of LDM-DOs, an ITS-S application process can unsubscribe from the subscription using the interface function of ASN.1 type `LDMunsubscribeRequest` specified in 6.7.4.5. This request is acknowledged with the interface function of ASN.1 type `LDMunsubscribeConfirm`.

A normative specification of the related procedure is presented in 7.1.3.7.

6.4.3.8 Notify updates of LDM-DOs

Upon successful subscription for updates of LDM-DOs, see 6.4.3.6, an ITS-S application process will be notified about updates of LDM-DOs with the interface function of ASN.1 type `LDMnotifyRequest` specified in 6.7.4.7. This notification is not acknowledged by the ITS-S application process.

A normative specification of the related procedure is presented in 7.1.3.8.

6.4.3.9 Second level filtering

Second level filtering is applied to values of attributes of LDM-DOs resulting from first level filtering performed in queries and notifications of updates, see 6.4.3.5 and 6.4.3.8. The return set from the first level filtering is further reduced to only those LDM-DOs that match the second level attribute filter. The filtered result will be returned in the interface functions of ASN.1 types `LDMqueryConfirm` and `LDMnotifyRequest` specified in 6.7.4.6 and 6.7.4.7, respectively.

The second level filter is a logical combination of one or more filter statements. A filter statement is a comparison statement in which an attribute from the LDM-DO is tested against a reference value. The

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 18750:2018