Draft ETSI EN 302 636-3 V1.1.2 (2014-03)

Intelligent Transport Systems (ITS);
Vehicular Communications;
GeoNetworking;
Part 3: Network Architecture

Reference
REN/ITS-0030034

Keywords
Autonomic Networking, ITS, network, safety

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This draft European Standard (EN) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

The present document is part 3 of a multi-part deliverable. Full details of the entire series can be found in part 1 [7].

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	18 months after doa

Introduction

The present document specifies the network architecture for communication-based Intelligent Transport Systems (ITS) using different ITS access technologies, such as ITS-G5. The network architecture provides - in combination with the description of scenarios - a basis for the technical specification of the networking and transport protocols, in particular for GeoNetworking and its related protocols.

The present document first introduces a generic, high-level system view of the network architecture and defines four basic deployment scenarios. Based on the system view, it identifies and describes the main network components and specifies network reference points among them. Central component of the architecture is the ITS station. For this component, an overview of its protocol architecture is given and different options of using the GeoNetworking protocol in combination with transport protocols and protocols of the IP suite are described. Finally, the present document defines frameworks for different aspects of networking and data transport, such as ad hoc communication, addressing, resource management and data congestion control, integration with protocols of the IP suite and others.

The network architecture is based on the ITS architecture specified in EN 302 665 [1] and represents the networking viewpoint of the overall architecture.

1 Scope

The present document specifies the network architecture of communications in Intelligent Transportation Systems (ITSC). The network architecture is focused on, but not limited to, vehicular communication. The architecture enables a wide range of ITS applications for road safety, traffic efficiency as well as for infotainment and business.

The present document defines the framework for network and data transport protocols that provide data exchange among ITS stations. A particular aspect is the GeoNetworking protocol that provides ad hoc and multi-hop communication over short-range wireless technologies utilizing geographical positions.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ETSI EN 302 665: "Intelligent Transport Systems (ITS); Communications Architecture".

[2] ISO/IEC 7498-1: "Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model".

[3] ETSI TS 102 637-1: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements".

[4] ETSI TS 102 637-2: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

[5] ETSI TS 102 637-3: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".

[6] ETSI EN 302 663: "Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band".

[7] ETSI EN 302 636-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements".

[8] ETSI EN 302 636-2: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 2: Scenarios".

[9] ETSI TS 102 636-4-1: "Intelligent Transport System (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality".

[10] ETSI TS 102 636-5-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol".

[11] ETSI TS 102 636-6-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols".

[12] ETSI TS 102 723 (all parts): "Intelligent Transport Systems (ITS); OSI cross-layer topics".

[13] ETSI TS 102 731: "Intelligent Transport Systems (ITS); Security; Security Services and Architecture".

[14] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".

[15] ISO/IEC 8802-2: "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements; Part 2: Logical Link Control".

[16] IETF RFC 791: "Internet Protocol".

[17] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

[18] IETF RFC 3775: "Mobility Support in IPv6".

[19] IETF RFC 768: "User Datagram Protocol".

[20] IETF RFC 793: "Transmission Control Protocol".

[21] IETF RFC 3963: "Network Mobility (NEMO) Basic Support Protocol".

[22] IETF RFC 5213: "Proxy Mobile IPv6".

[23] IETF RFC 5648: "Multiple Care-of Addresses Registration".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Recommendation ITU-R M.687-2: "International Mobile Telecommunications 2000 (IMT-2000)".

[i.2] IETF RFC 3753: "Mobility Related Terminology".

[i.3] 3GPP: "UMTS Standard, Release 08 Specification".

NOTE: Available at: http://www.3gpp.org.

[i.4] IETF RFC 4213: "Basic Transition Mechanisms for IPv6 Hosts and Routers".

[i.5] IETF RFC 2185: "Routing Aspects of IPv6 Transition".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EN 302 665 [1], ISO/IEC 7498-1 [2] and the following apply:

access network gateway: router at the edge of a network that connects an ITS station-internal network to the ITS access network, the public access network, and the private access network

access router: IPv6 router that acts as point of attachment and provides access to other networks, such as to the ITS access network

NOTE: The definition is taken from RFC 3753 [i.2] and adapted to the ITS network architecture.

ad hoc network: wireless networks based on self-organization without the need for a coordinating infrastructure

ad hoc router: router that is associated with the ITS ad hoc network and executes an ad hoc networking protocol

Application Unit (AU): physical unit in an ITS station that executes applications and uses the communication services of a communication & control unit (CCU)

Communication and Control Unit (CCU): physical communication unit located in an ITS station that implements communication protocols and provides communication services

GeoNetworking: network service that utilizes geographical positions and provides ad hoc communication without the need for a coordinating communication infrastructure

GeoNetworking protocol: network protocol that provides the GeoNetworking service

ITS access network: communication network that interconnects roadside ITS stations among each other in an ITS specific way and optionally interconnects them to the core network (e.g. the Internet)

ITS ad hoc network: special type of mobile ad hoc network in the ITS architecture that enables self-organized communication among ITS stations without the need for a coordinating communication infrastructure

ITS operational support service: service for operation of the ITS, such as the provision of security credentials to users and vehicle drivers

ITS station internal network: network that interconnects the different components of an ITS station

legacy roadside infrastructure: road infrastructure, e.g. road sensors, loops, networks, switches, router, processing entities, etc.

legacy services: legacy Internet services, such as WWW, email, Internet access, file transfer, etc.

mobile network: entire network, moving as a unit, which dynamically changes its point of attachment to the Internet and thus its reachability in the topology

mobile router: IPv6 router that acts as gateway between a IPv6 mobile network and another IP-based network, and capable of changing its point of attachment to the network, moving from one link to another link

private access network: network that provides data services to a closed user group for a secured access to another system

proprietary local network: communication network attached to an ITS station, for example a controller area network (CAN) in a vehicle or a network of roadside legacy infrastructure

public access network: network that provides access to general purpose networks that are publicly accessible

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in EN 302 665 [1], ISO/IEC 7498-1 [2] and the following apply:

AU	Application Unit
CAN	Controller Area Network
CCU	Communication and Control Unit
DCC	Decentralized Congestion Control
GPRS	General Packet Radio Service
IMT	International Mobile Telecommunications
IP	Internet Protocol
ITSC	ITS Communications
NEMO	Network Mobility
PDCP	Packet Data Convergence Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
WIMAX™	Worldwide Interoperability for Microwave Access
WWW	World Wide Web

4 Network architecture for ITS stations

The network architecture comprises external and internal networks. External networks interconnect ITS stations among each other or connect ITS stations to other network entities. The following external networks are identified:

- ITS ad hoc network.
- Access network (ITS access network, public access network, private access network).
- Core network (e.g. the Internet).

Additionally, an ITS station can have an internal network that interconnects the components of the ITS station.

The different networks shall provide support for at least one of the use cases of road safety, traffic efficiency, infotainment and business applications. However, it is presumed that the communication within a single network does not meet all the requirements of all applications and use cases. Instead combinations of networks are envisioned, in which multiple ITS access and networking technologies are applied.

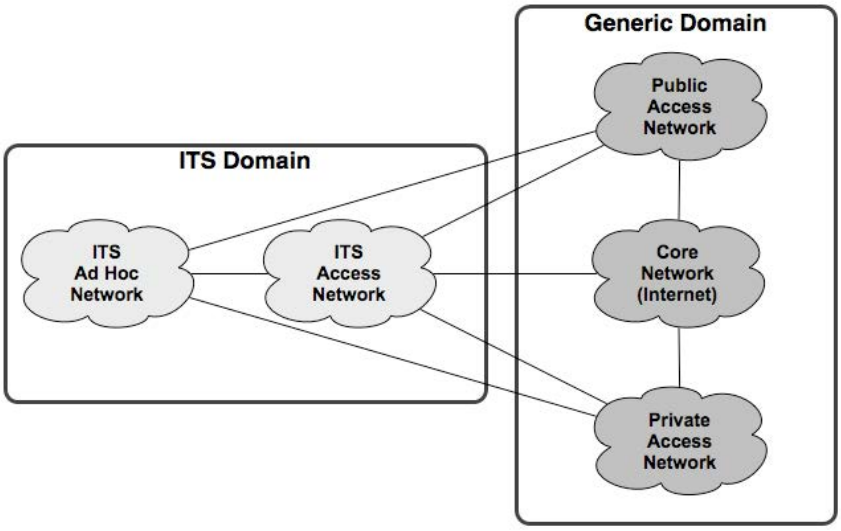

Figure 1: External networks involved in the ITS architecture and their interconnections

Figure 1 represents the highest level of abstraction of the ITS network architecture, where the external networks, represented by clouds are connected. The networks can be categorized into an ITS domain and a generic domain as specified in EN 302 665 [1]. The external networks can be described as follows:

The *ITS ad hoc network* enables ad hoc communication among vehicle, roadside and personal ITS stations. The communication is based on wireless technologies that provide a short communication range (referred to as "short-range wireless technology") and allow for mobility of the ITS stations forming arbitrary network topologies without the need for a coordinating communication infrastructure. An example of an *ITS ad hoc network* is a network of vehicle, roadside and personal ITS stations interconnected by ITS-G5 wireless technology as defined in EN 302 663 [6].

An *ITS access network* is a dedicated network that provides access to specific ITS services and applications and can be operated by a road operator or other operators. The ITS access network also interconnects roadside ITS stations and provides communication in between these as well as among vehicle ITS stations via the roadside ITS stations that are interconnected in the *ITS access network*. This local network can then enable the vehicle ITS stations to communicate via a roadside infrastructure communication network instead directly in ad hoc mode. As an example, an ITS access network can connect roadside ITS stations along a highway with a central ITS station (e.g. a road traffic management centre). In the case that short-range wireless technology is used for communication via roadside ITS stations, the connectivity to the *ITS access network* is typically provided intermittently.

A *public access network* provides access to general purpose networks that are publicly accessible. An example is an IMT-2000 network as outlined in Recommendation ITU-R M.687-2 [i.1] that connects vehicle ITS stations to the Internet and provides mobile Internet access.

A *private access network*, in contrast to a public access network, provides data services to a closed user group for a secured access to another network. For example, a *private access network* can connect vehicle ITS stations to a company's intranet.

The access networks and the core network provide access to various services:

- legacy services, such as WWW, email and many others;
- ITS services provided by road traffic management centres and backend services;
- ITS operational support services required to operate the ITS, such as security services.

Core component of the architecture is the ITS station, which has two main roles: in its first role, the ITS station is a network node and acts as a communication source or sink. Likewise an ITS station can be a forwarder of data, e.g. in the *ITS ad hoc network*. In its second role, the ITS station is placed at the network edge and connect the different networks via an *ITS station internal network* (see Figure 1).

ITS stations shall be able to communicate via at least one of the following means (see Figure 2):

a) via an ITS ad hoc network;

b) via an ITS access network;

c) via a public access network;

d) via a private access network;

e) via one of the access networks into the core network (e.g. the Internet).

In addition to the networks listed above, an ITS station can also be attached to *proprietary local networks* of e.g. vehicle ITS sub-systems and roadside ITS sub-system as presented in EN 302 665 [1]. Typical examples are:

- Controller Area Network (CAN) in a vehicle ITS sub-system.
- Legacy roadside infrastructure in a roadside ITS sub-system.

However, these proprietary networks are outside the scope of the present document.

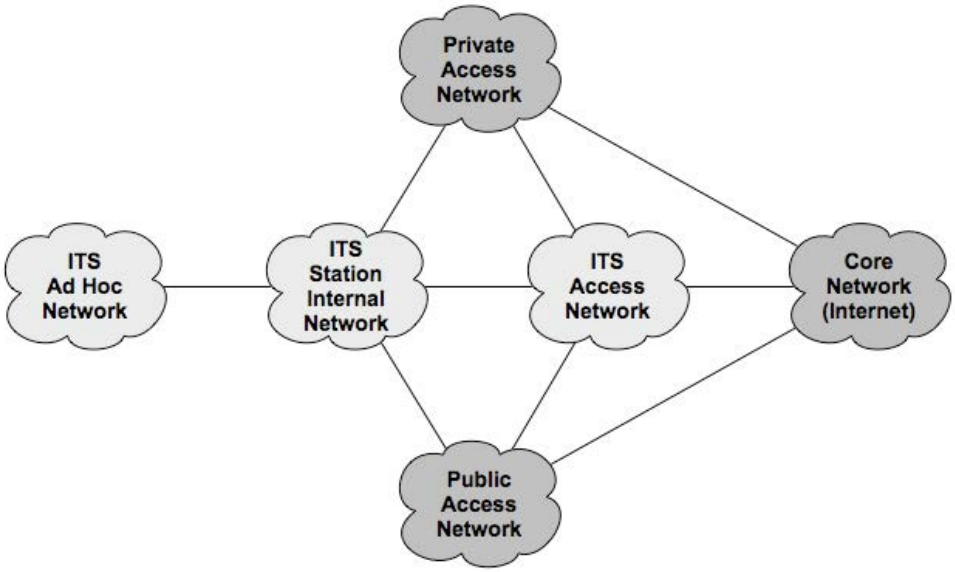

Figure 2: High-level network architecture

5 Deployment scenarios of the generic network architecture

The ITS network architecture can be deployed in different scenarios to adapt to specific economical and regulatory conditions and to facilitate a gradual introduction of ITS. Basically, a deployment scenario is a subset of the overall architecture (see Figure 2) created by a combination of the different network types in support of the communication scenarios specified in EN 302 636-2 [8].

Four basic deployment scenarios can be defined. The basic deployment scenarios can further be extended to hybrid scenarios that combine two or more deployment scenarios. These combinations also include scenarios in which a network is connected to more than a single network simultaneously.

Scenario A establishes an ITS ad hoc network, which can be connected via an ITS access network to the core network (e.g. the Internet) (see Figure 3). Deployment scenario B represents an ITS access network, which can be connected to the core network (e.g. the Internet) (see Figure 4). Deployment scenario C is based on a public access network, which can also provide connectivity to the core network (e.g. the Internet) (see Figure 5). Deployment scenario D uses a private access network to connect to other networks or the core network (e.g. the Internet) (see Figure 6).

Figure 3: Deployment scenario A: Ad hoc-centric

In Figure 4, the ITS access network connects roadside ITS stations to each other and provides connectivity to a core network (e.g. the Internet). Optionally, the ITS access network can also be replaced by a public or private access network.

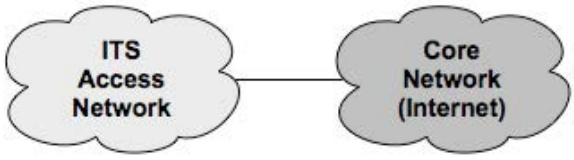

Figure 4: Deployment scenario B: ITS access network-centric

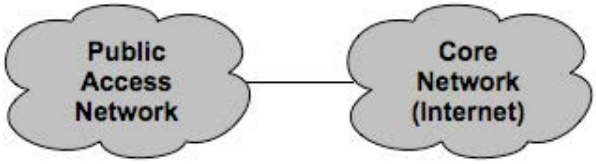

Figure 5: Deployment scenario C: Public access network-centric

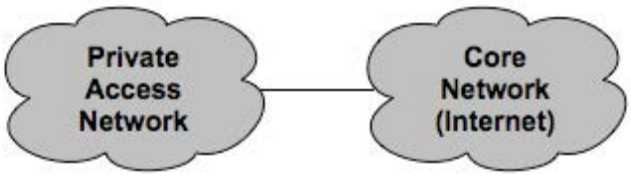

Figure 6: Deployment scenario D: Private access network-centric

6 Components of the network architecture

6.1 General

Main component of the network architecture is the ITS station as specified in EN 302 665 [1]. The following types of ITS stations are identified:

- vehicle ITS station;
- personal ITS station;
- roadside ITS station;
- central ITS station.

In addition to these instantiations, the ITS-S Border Router as specified in EN 302 665 [1] interconnects networks in the ITS domain with networks in the generic domain. Additionally to the ITS station component, the present document introduces specific network components related to IPv6 communication as outlined in RFC 3753 [i.2], i.e.:

- ad hoc router;
- mobile router;
- access router; and
- access network gateway;

that will be defined below.

6.2 Sub-components of vehicle ITS stations and roadside ITS stations

Vehicle ITS stations and roadside ITS stations consist of two types of sub-components, the *Communication & Control Unit (CCU)* and the *Application Unit (AU)* (Figure 7). In general, a CCU executes a communication protocol stack. An AU runs a single or a set of applications and utilizes the CCU's communication capabilities.

In a possible implementation, the CCU executes the ITS access technology, ITS network & transport, and the ITS facilities layers, whereas the ITS application layer resides in the AU. The distinction between AU and CCU is logical; all layers can also be implemented in a single physical unit.

NOTE: The components of a personal ITS station and central ITS station will be refined at a later stage of the network architecture definition.

The CCU shall be equipped with at least a single ITS external communication interface to provide connectivity to the *ITS ad hoc network* or the different access networks (*ITS access network, public access network, private access network)*. The CCU and the AU can be equipped with one or multiple ITS internal communication interfaces. Moreover, an AU can have an external communication interface ("Gateway Interface" in Figure 7) for access to the *proprietary local network*.

The ITS internal communication interface shall connect AUs with CCUs, AUs with other AUs, and CCUs with other CCUs via the ITS station-internal network. AUs and CCUs can form a *mobile network* as outlined in RFC 3753 [i.2], where the AUs obtain connectivity to the networks via the external communication interface of the CCU. AU and CCU can reside in a single physical unit.

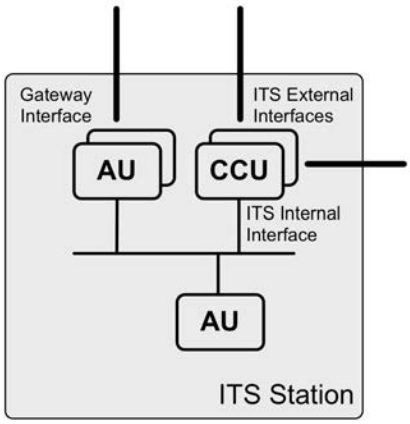

Figure 7: Sub-components of a vehicle ITS station and a roadside ITS station

The CCU can be further sub-divided into logical network components of different types operating at the network layer:

- ad hoc router;
- mobile router;
- access router; and
- access network gateway;

that are responsible for routing and forwarding of packets in the corresponding networks.

An *ad hoc router* shall be associated with the ITS ad hoc network and executes an ad hoc networking protocol, such as the GeoNetworking protocol.

A *mobile router* is a network component of the vehicle ITS station and shall provide IP connectivity of the ITS station internal network to an *access router*. The mobile router is capable of changing its point-of-attachment to the access network.

The *access router* given in RFC 3753 [i.2] is a specific ITS-S router as specified in EN 302 665 [1] based on IP. It offers IP connectivity to ITS stations and acts as a default router to the ITS stations it is currently serving. The access router is part of an access network, such as the *ITS access network*.

An *access network gateway* as outlined in RFC 3753 [i.2] is a specific ITS-S border router as specified in EN 302 665 [1] based on IP. It connects:

- an ITS internal network and an access network;
- an access network and the core network.

6.3 Network connectivity among ITS stations

The following Figure 8 to Figure 11 show the connectivity among the ITS stations, where the link between the ITS stations represents an abstraction of the respective networks. The ITS stations are interconnected to ITS stations of different type (e.g. the vehicle ITS station and the roadside ITS station in Figure 8), but also to ITS stations of the same type (e.g. vehicle ITS stations among each other as in Figure 8).

In Figure 8 to Figure 11 below, the roadside ITS station acts as point of attachment to other networks for the vehicle ITS stations and roadside ITS station. The ITS-S border router as defined in EN 302 665 [1] connects access networks with the core network (e.g. the Internet), i.e. the ITS access network (Figure 8 and Figure 9), the public access network (Figure 10) and the private access network (Figure 11). For IP-based networks, the ITS-S border router is an access network gateway as outlined in RFC 3753 [i.2].

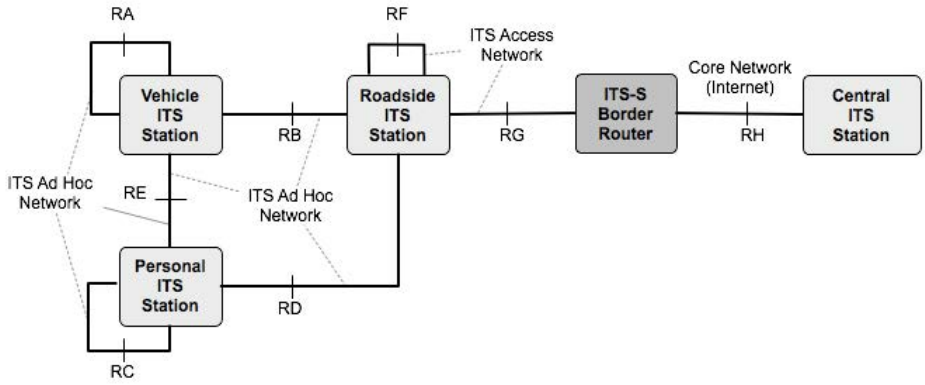

Figure 8: Connectivity among ITS stations for deployment scenario A

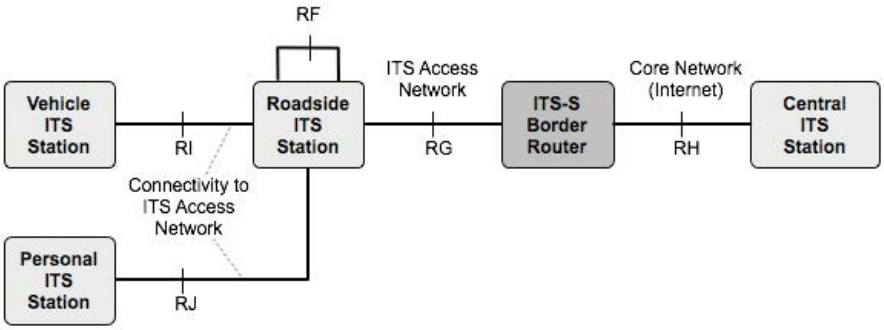

Figure 9: Connectivity among ITS stations for deployment scenario B

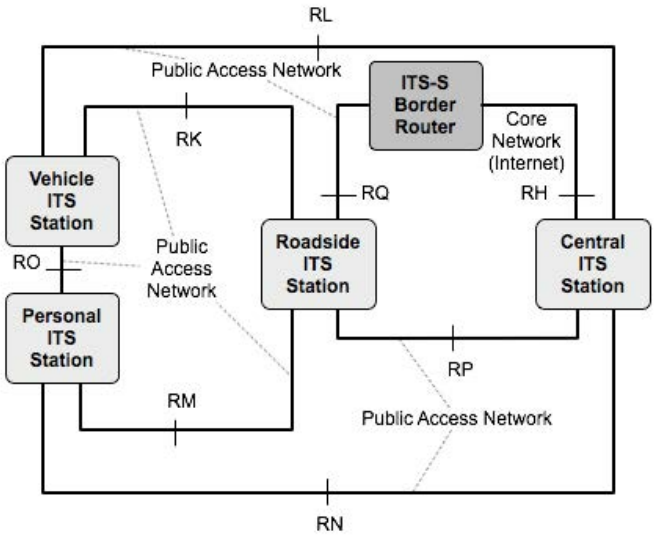

Figure 10: Connectivity among ITS stations for deployment scenario C

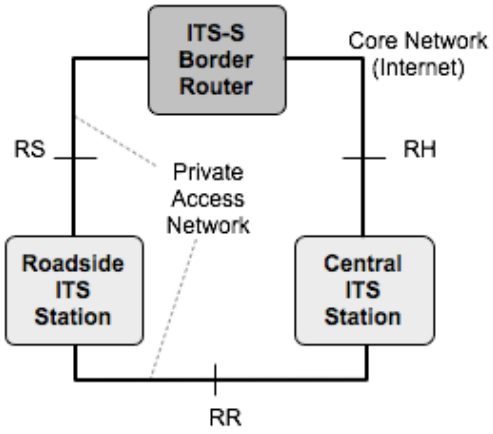

Figure 11: Connectivity among ITS stations for deployment scenario D

6.4 Network reference points

The following network reference points are defined (Figure 8 to Figure 11):

- R_A Reference point between vehicle ITS stations via the ITS ad hoc network.
- R_B Reference point between vehicle ITS station and roadside ITS station via the ad hoc network.
- R_C Reference point between personal ITS stations via the ITS ad hoc network.
- R_D Reference point between personal ITS station and roadside ITS station via the ad hoc network.
- R_E Reference point between vehicle ITS station and personal ITS station via the ITS ad hoc network.
- R_F Reference point between roadside ITS stations via the ITS access network.
- R_G Reference point between roadside ITS station and ITS-S Border Router via the ITS access network.
- R_H Reference point between central ITS station and ITS-S Border Router via the core network (e.g. the Internet).
- R_I Reference point between vehicle ITS station and roadside ITS station via the ITS access network.
- R_J Reference point between personal ITS station and roadside ITS station via the ITS access network.
- R_K Reference point between vehicle ITS station and roadside ITS station via the public access network.
- R_L Reference point between vehicle ITS station and central ITS station via the public access network.
- R_M Reference point between personal ITS station and roadside ITS station via the public access network.
- R_N Reference point between personal ITS station and central ITS station via the public access network.
- R_O Reference point between vehicle ITS station and personal ITS station via the public access network.
- R_P Reference point between roadside ITS station and central ITS station via the public access network.
- R_Q Reference point between roadside ITS station and ITS-S Border Router via the public access network.
- R_R Reference point between roadside ITS station and central ITS station via the private access network.

- R_S Reference point between roadside ITS station and ITS-S Border Router via the private access network.

7 ITS station protocol architecture

7.1 Protocol stack overview

The protocol stack of an ITS station (Figure 12) specified in EN 302 665 [1] basically follows the ISO/OSI reference model defined in ISO/IEC 7498-1 [2] and defines three horizontal protocol layers, two vertical protocol entities and the ITS applications on top. This clause gives an overview of the protocol stack and focuses on networking aspects. The horizontal protocol layers are:

- **ITS access technologies** layer covers various communication media and related protocols for the physical and data link layers. The access technologies are not restricted to specific type of media, though most of the access technologies are based on wireless communication. The access technologies are used for communication inside of an ITS station (among its internal components) and for external communication (for example with other ITS stations). For external communication, some of the ITS access technologies represent complete, non-ITS specific communication systems (such as GPRS, UMTS, WiMAX™) that are regarded as "logical links" over which ITS data is transparently transported.

- The **ITS network & transport** layer comprises protocols for data delivery among ITS stations and from ITS stations to other network nodes, such as network nodes in the core network (e.g. the Internet). ITS network protocols particularly include the routing of data from source to destination through intermediate nodes and the efficient dissemination of data in geographical areas. ITS transport protocols provide the end-to-end delivery of data and, depending on requirements of ITS facilities and applications, additional services, such as reliable data transfer, flow control and congestion avoidance. A particular protocol in the ITS network & transport layer is the Internet protocol IP version 6 (IPv6). The usage of IPv6 includes the transmission of IPv6 packets over ITS network protocols, dynamic selection of ITS access technologies and handover between them, as well as interoperability issues of IPv6 and IPv4.

- The **ITS facilities** layer provides a collection of functions to support ITS applications. The facilities provide data structures to store, aggregate and maintain data of different type and source (such as from vehicle sensors and from data received by means of communication). As for communication, ITS facilities enable various types of addressing to applications, provide ITS-specific message handling and support establishment and maintenance of communication sessions. An important facility is the management of services, including discovery and download of services as software modules and their management in the ITS station.

The **ITS applications** on top of the protocol layers realize the use cases for road safety, traffic efficiency, infotainment and business. They use the ITS station protocol stack.

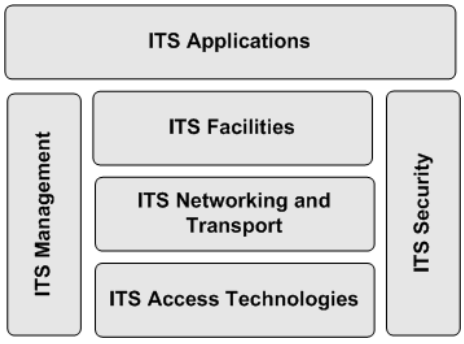

Figure 12: Reference protocol stack of an ITS station

The two vertical protocol entities are:

- **ITS management** entity is responsible for configuration of an ITS station, cross-layer information exchange among the different layers and others tasks.

- **ITS security** entity provides security and privacy services, including secure messages at different layers of the communication stack, management of identities and security credentials, and aspects for secure platforms (firewalls, security gateway, tamper-proof hardware).

NOTE: Figure 12 shows a simplified version of the ITS station reference architecture specified in EN 302 665 [1].

7.2 Protocols of the ITS networking and transport layer

The ITS networking and transport layer comprises several networking and transport protocols (Figure 13). In detail an ITS station can execute the following protocols at the ITS networking and transport layer:

- **GeoNetworking** protocol. For usage of the GeoNetworking over different ITS access technologies, the specification of the protocol is split into a media-independent part and a media-dependent part (potentially multiple parts), such as for ITS-G5 specified in EN 302 663 [6].
- **Transport protocols** over GeoNetworking, such as the Basic Transport Protocol defined in TS 102 636-5-1 [10] and other GeoNetworking transport protocols as they may be defined later.
- **Internet protocol IP version 6** as defined in RFC 2460 [17] with IP mobility support specified in RFC 3775 [18] and optionally support for network mobility (NEMO) as defined in RFC 3963 [21] or other approaches depending on the deployment scenario.
- **Internet protocol IP version 4** for transition to IPv6 as specified in RFC 791 [16].
- **User Datagram Protocol UDP** as defined in RFC 768 [19].
- **Transmission Control Protocols TCP** as specified in RFC 793 [20].
- **Other network protocols.**
- **Other transport protocols,** such as SCTP.

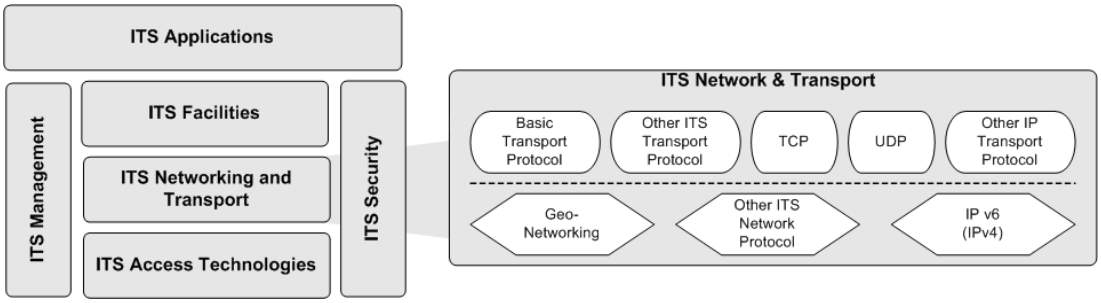

Figure 13: Details of the ITS networking and transport layer

The networking and transport protocols can operate over various ITS access technologies as specified in EN 302 665 [1]. For specific ITS access technologies, however, the usage of networking and transport protocols can be restricted.

7.3 Assembly of networking and transport protocols in the ITS station protocol stack

7.3.1 Overview

For protocol stacks involving the GeoNetworking protocol and IPv6 protocols shall be assembled in one of the following ways described in clause 7.3.2, clause 7.3.3 and clause 7.3.4. The protocol stacks for other network protocols are described in clause 7.3.5.

For the GeoNetworking protocol, the underlying ITS access technologies are limited to short-range wireless technologies, such as ITS-G5 defined in EN 302 663 [6].

7.3.2 GeoNetworking protocol stack

The GeoNetworking protocol stack may be assembled with the GeoNetworking protocol and ITS-specific transport protocols as envisaged in TS 102 636-5-1 [10] at the top of the GeoNetwork protocol as depicted in Figure 14.

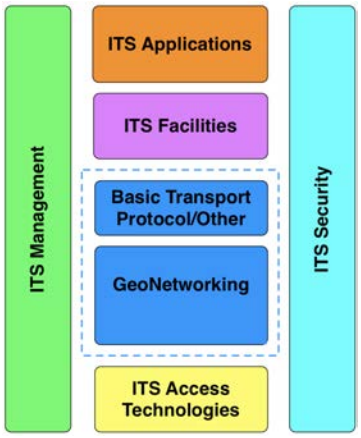

Figure 14: GeoNetworking protocol stack in an ITS station

7.3.3 IPv6 stack

The IPv6 stack may be assembled with the IPv6 protocol and related transport protocols UDP defined in RFC 768 [19], TCP defined in RFC 793 [20] and others as depicted in Figure 15.

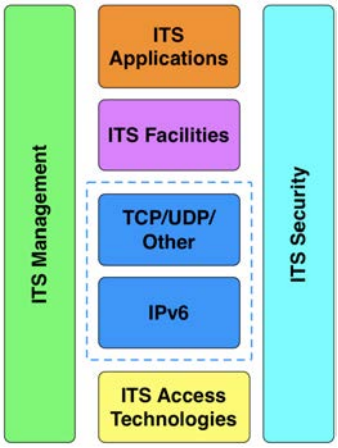

Figure 15: IPv6 stack in an ITS station

7.3.4 Combination of the GeoNetworking protocol and IPv6

This protocol stack combines the stacks in clause 7.3.2 and clause 7.3.3. In this protocol stack (Figure 16), IP shall run at the top of the GeoNetworking protocol as specified in TS 102 636-6-1 [11] or directly at the top of the ITS access technologies.

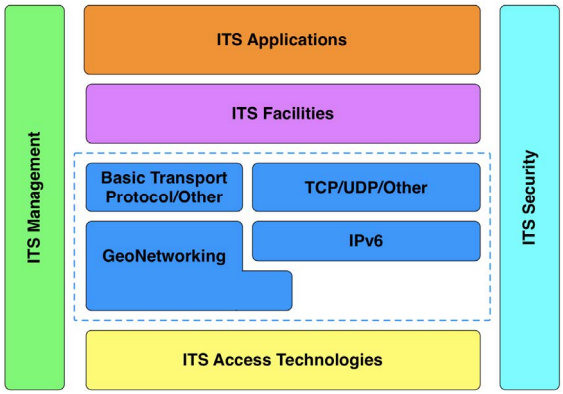

Figure 16: Combined GeoNetworking and IPv6 stack in an ITS station

7.3.5 Protocol stacks for other network protocols

Further protocol stacks can be defined for other network protocols.

In order to meet application and system requirements, the usage of other network protocols in parallel to the protocol stacks defined in clause 7.3.2, clause 7.3.3 and clause 7.3.4 can be restricted.

8 Interfaces and service access points

The ITS networking and transport layer provides services to the ITS Facility layer. In order to provide its service, the ITS networking and transport layer uses services from other layers and entities, namely the ITS access technology layer, ITS management entity and ITS security entity. In an ITS station, the following four interfaces are defined that are relevant for the ITS network & transport layer (Figure 17):

- NF Interface between the ITS networking and transport layer and the ITS facility layer.
- IN Interface between the ITS access technology layer and the ITS networking and transport layer.
- MN Interface between the ITS management entity and the ITS networking and transport layer.
- SN Interface between the ITS security entity and the ITS networking and transport layer.

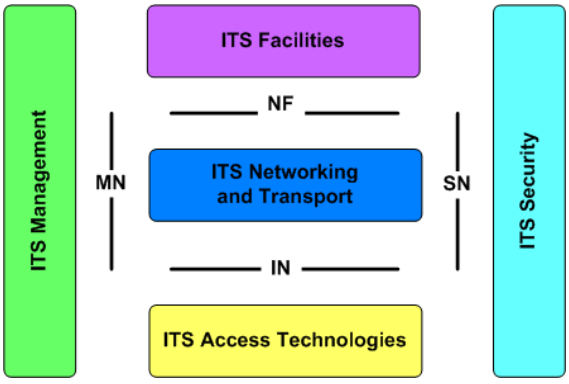

Figure 17: Interfaces of the ITS station relevant for the ITS network & transport layer

The services of the protocols are made available through service access points (SAPs) as specified in the respective parts of TS 102 723 [12]. The ITS networking and transport layer shall support at least one of the following SAPs for the NF interface (Figure 18):

- $SAP_{GeoAware}$ SAP for protocols of the ITS facility layer that can utilize the capabilities of the GeoNetworking protocol, such as addressing geographical areas and are not based on IP. Examples for such protocols of the ITS facility layer are described in TS 102 637-1 [3], TS 102 637-2 [4], TS 102 637-3 [5], such as the *Cooperative Awareness Message (CAM)* protocol and the *Decentralized Environmental Notification Message (DENM)* protocol.
- SAP_{UDP} SAP for Internet-based ITS applications and facilities that utilize UDP as defined in RFC 768 [19].
- SAP_{TCP} SAP for Internet-based ITS applications and facilities that utilize TCP as defined in RFC 793 [20].

NOTE 1: SAPs for other transport protocols, such as SCTP may be defined if needed.

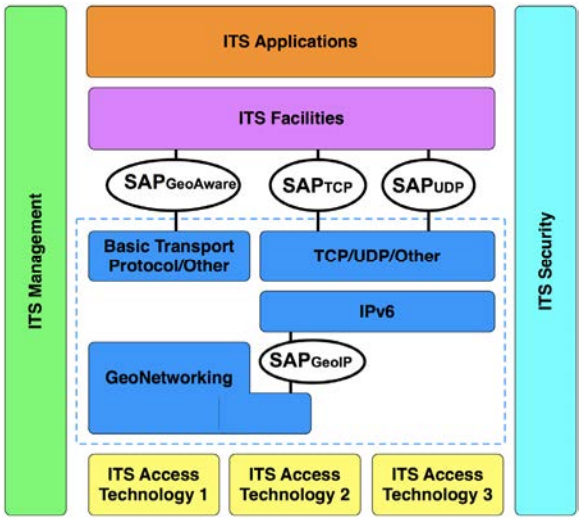

Figure 18: SAPs offered by the ITS networking and transport layer

In addition, the ITS network & transport layer can support a SAP inside the ITS networking and transport layer (Figure 18), offered by the GeoNetworking protocol to IPv6:

- SAP_{GeoIP} SAP for IPv6 packet transport over GeoNetworking (TS 102 636-4-1 [9]).

The GeoNetworking protocol uses the following SAPs defined by other ITS protocol layers (Figure 19):

- Via the MN interface
  - $SAP_{GeoConfig}$ SAP for configuration of GeoNetworking.
  - $SAP_{GeoXlayer}$ SAP for cross-layer information exchange.

NOTE 2: These SAPs are not defined in the ITS management layer (yet).

- Via the SN interface
  - SAP_{GeoSec} SAP between the GeoNetworking and the corresponding security layer.

NOTE 3: These SAPs are not defined in the ITS security layer (yet).

- Via the IN interface
  - SAP_{8022} SAP offered by access technologies based on 802.2 LLC/SNAP. The SAP is specified in ISO/IEC 8802-2 [15].
  - SAP_{UMTS} SAP between the IPv6 layer and UMTS UE (PDCP) as defined in 3GPP [i.3].

NOTE 4: The SAPs to the ITS access technologies are technology-specific (or at least specific to groups of technologies, such as 802-type technologies).

NOTE 5: SAPs offered by other ITS access technologies need to be defined in the future.

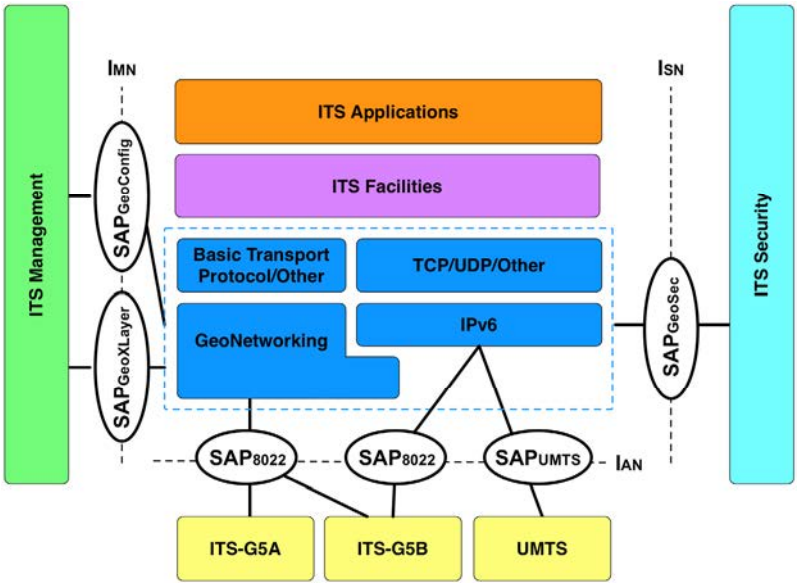

Figure 19: SAPs used by the ITS network & transport layer

9 Framework for networking and transport protocols

This clause defines high-level logical functions to be considered in the design of ITS networking and transport protocols.

9.1 GeoNetworking functional requirements

9.1.1 Ad hoc networking

GeoNetworking shall provide ad hoc networking based on geographical addressing and geographical routing between ITS stations using short-range wireless technology. It shall allow the addressing of ITS stations based on their individual network addresses and also facilitate the addressing of geographical areas. For routing, GeoNetworking shall support point-to-point and point-to-multipoint communication, as well as the distribution of data packets in geographical areas, i.e. to all nodes in a geographical area (GeoBroadcast) or to any node in a geographical area (GeoAnycast).

9.1.2 Addressing

For packet transport, Network and transport layer of an ITS-Station shall be addressed by network addresses. The address type is protocol-specific and shall include at least GeoNetworking addresses, IPv6 addresses and should include IPv4 addresses. GeoNetworking shall apply a particular concept of geographical addressing, i.e. it shall allow for communication with an ITS station by its network address and geographical position in the ad hoc network. Likewise, it shall also be able to address ITS stations in geographical areas. IP addresses shall be assigned to an ITS station based on existing approaches (e.g. by auto-configuration depending on the network scenario). An ITS station can have multiple IP addresses assigned in order to cope with IP mobility issues. Network addresses of ITS stations can change to alleviate privacy issues.

NOTE: The concept of changing pseudonyms is being defined by TC ITS WG5.

9.1.3 Resource management and decentralized data congestion control

ITS applications, in particular safety-related applications, have high requirements on the reliability and the delay of the data transmission. Considering the limitations of the ITS-related frequency bands, the data load on the wireless channels can exceed the available network resources and capacity in some situations. Decentralized congestion control (DCC) shall limit the channel load and shall ensure network stability, throughput efficiency and fair resource allocation to ITS stations. DCC requires mechanisms on all layers of the protocol stack and a harmonization of these mechanisms among the layers. The GeoNetworking protocol shall allow the exchange of information among ITS-Ss to support the DCC operation at other layers.

9.1.4 Integration of GeoNetworking and IPv6

The ITS ad hoc network shall provide the transport of IPv6 packets enhanced by GeoNetworking for communication among ITS stations. The delivery of IPv6 packets shall be achieved by *IPv6 in GeoNetworking header tunnelling,* i.e. encapsulation of IPv6 packets (header and payload) into GeoNetworking packet headers and routing of the encapsulated packets by the GeoNetworking protocol. From the IPv6 layer perspective, the ITS stations shall appear as attached to the same IPv6 "link". For different communication scenarios, such for ad hoc networking among ITS stations without connectivity to a communication infrastructure or for communication with IPv6 nodes in the Internet, when access to the communication infrastructure is available, specific mechanisms for IPv6 address configuration shall be applied.

When vehicle ITS stations have access to a communication infrastructure, IPv6 support over GeoNetworking should be enhanced with solutions for IP mobility support. Those solutions achieve global reachability of IP nodes and IP session continuity. Different approaches for IP mobility can be applied, such as RFC 3775 [18], RFC 5213 [22] and RFC 5648 [23]. As an ITS station can include a set of attached devices (AUs) and form an IPv6 mobile network opposed to a single "IPv6 node", *NEMO Basic Support* as specified in RFC 3963 [21] should be applied to maintain ongoing sessions during IP handovers.

9.1.5 Backward compatibility to IPv4

In principle, the communication using the Internet protocol in ITS is based on IP version 6. Backward compatibility from IPv6 to IPv4 is needed as required for legacy Internet applications that require IPv4, and *Public Access Networks* that are capable of IPv4 only. In order to achieve the backward compatibility, standard mechanisms should be applied, such as the usage of IP4/IPv6 capable addresses and IPv4 in IPv6 tunnels, or dual-stack IP (see RFC 4213 [i.4] and RFC 2185 [i.5]).

9.1.6 Usage of multiple ITS access technologies

GeoNetworking shall be capable for routing of packets over different types of short-range wireless technologies. In case an ITS station is equipped with multiple communication interfaces of different technologies, the GeoNetworking protocol should provide mechanisms to choose the communication interface based on policies.

9.1.7 Security and privacy protection

In order to provide secure communication, including authentication, authorization, integrity and non-repudiation, the GeoNetworking protocol shall support cryptographic protection based on digital signatures and certificates. Additionally, the networking operations shall be protected by plausibility checks, rate limitation and trustworthiness assessment. Furthermore, the anonymity of users shall be protected by usage of anonymous identifiers by means of pseudonyms and anonymous certificates.

More details are described in TS 102 731 [13] and TS 102 940 [14].

9.2 Other protocol stacks

Other protocol stacks are out of scope of the present document.

Annex A (informative): Bibliography

ETSI EN 302 931: "Intelligent Transport Systems (ITS); Vehicular Communications; Geographical Area Definition".

COMeSafety Deliverable 3.1 - Version 2.0 - March 2009: "European ITS Communication Architecture - Overall Framework - Proof of Concept Implementation".

PRE-DRIVE C2X Deliverable 1.4 - Version 1.2 - August 2009: "Refined Architecture".

GeoNet Deliverable 1.2 - Version 1.2 - June 2010: "Final GeoNet Architecture Design".

GeoNet Deliverable 2.2 - Version 1.1 - January 2010: "Final GeoNet Architecture Specification".

History

Document history		
V1.1.1	March 2010	Publication as TS 102 636-3
V1.1.2	March 2014	EN Approval Procedure AP 20140716: 2014-03-18 to 2014-07-16