



TECHNICAL SPECIFICATION

**Intelligent Transport Systems (ITS);  
Security;  
ITS communications security architecture and  
security management**

PREVIEW  
Full standard available at  
https://standards.iteh.ai/catalog/standards/sist/26fe023c-9ed7-4292-a3d8-35d9ceb04e8/etsi-ts-102-940-v1.2.1-2016

---

**Reference**

RTS/ITS-00532

---

**Keywords**

interoperability, ITS, management, security

**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/standards-search>

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  
<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:  
<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

---

**Copyright Notification**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.  
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.  
All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.  
**3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.  
**GSM®** and the GSM logo are Trade Marks registered and owned by the GSM Association.

# Contents

Intellectual Property Rights .....	5
Foreword.....	5
Modal verbs terminology.....	5
1 Scope .....	6
2 References .....	6
2.1 Normative references .....	6
2.2 Informative references.....	7
3 Definitions and abbreviations.....	7
3.1 Definitions.....	7
3.2 Abbreviations .....	7
4 ITS reference architecture .....	8
4.1 Background .....	8
4.2 ITS applications groups.....	10
4.2.1 ITS applications groups and their communication characteristics.....	10
4.2.2 Cooperative awareness .....	13
4.2.3 Static local hazard warning.....	13
4.2.4 Interactive local hazard warning.....	14
4.2.5 Area hazard warning.....	14
4.2.6 Advertised services.....	15
4.2.7 Local high-speed unicast service .....	15
4.2.8 Local multicast service .....	16
4.2.9 Low-speed unicast service.....	16
4.2.10 Distributed (networked) service.....	17
4.2.11 Multiple Applications .....	17
4.3 Security requirements of ITS application groups.....	17
4.3.1 Security requirements of cooperative awareness.....	17
4.3.1.1 Authentication and Authorization.....	17
4.3.1.2 Confidentiality .....	18
4.3.1.3 Privacy .....	18
4.3.2 Security requirements of static local hazard warnings.....	18
4.3.2.1 Authentication and Authorization .....	18
4.3.2.2 Confidentiality and Privacy.....	18
4.3.3 Security requirements of interactive local hazard warnings .....	18
4.3.3.1 Authentication and Authorization .....	18
4.3.3.2 Confidentiality and Privacy.....	18
4.3.4 Security requirements of area hazard warnings .....	19
4.3.4.1 Authentication and Authorization .....	19
4.3.4.2 Confidentiality and Privacy.....	19
4.3.5 Security requirements of advertised services.....	19
4.3.5.1 Authentication and Authorization .....	19
4.3.5.2 Confidentiality and Privacy.....	19
4.3.6 Security requirements of other services.....	19
4.3.7 Security requirements of multiple applications.....	19
4.3.7.1 Authentication and Authorization .....	19
4.3.7.2 Confidentiality and Privacy.....	19
5 ITS communications security architecture .....	20
5.1 ITS station communications security architecture.....	20
5.2 Security services.....	21
5.3 ITS security functional model .....	23
6 ITS station security management .....	27
6.1 Basic principles .....	27
6.2 Guidelines for establishing enrolment trust requirements .....	28
6.3 Trust and privacy management .....	29

6.4	Access control .....	30
6.5	Identity management .....	30
6.6	Confidentiality .....	31
<b>Annex A (informative): Security Management System Functional Overview .....</b>		<b>32</b>
A.1	Objective of this annex .....	32
A.2	Security Management system architecture .....	32
A.3	Security functional elements .....	33
A.4	Security reference points .....	34
History .....		38

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)

Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/26fe023c-9ed7-4292-a3d8-35d9ce6c1de8/etsi-ts-102-940-v1.2.1-2016-11>

---

## 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 (<https://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 Technical Specification (TS) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

---

## Modal verbs terminology

In the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"must" and "must not" are **NOT** allowed in ETSI deliverables except when used in direct citation.

iTeh STANDARD PREVIEW  
(standards.iteh.ai)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/102-940-v1-2-1-9ed7-4292-a3d8-35d9ce6c1de8/etsi-ts-102-940-v1-2-1-2016-11>

---

# 1 Scope

The present document specifies a security architecture for Intelligent Transport System (ITS) communications. Based upon the security services defined in ETSI TS 102 731 [4], it identifies the functional entities required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in ETSI EN 302 665 [1].

The present document also identifies the roles and locations of a range of security services for the protection of transmitted information and the management of essential security parameters. These include identifier and certificate management, PKI processes and interfaces as well as basic policies and guidelines for trust establishment.

---

## 2 References

### 2.1 Normative 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 referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <https://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.

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] ETSI EN 302 637-2: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".
- [3] ETSI EN 302 637-3: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".
- [4] ETSI TS 102 731: "Intelligent Transport Systems (ITS); Security; Security Services and Architecture".
- [5] ETSI TS 102 941: "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".
- [6] ETSI TS 102 942: "Intelligent Transport Systems (ITS); Security; Access Control".
- [7] ETSI TS 102 943: "Intelligent Transport Systems (ITS); Security; Confidentiality services".
- [8] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".
- [9] ETSI TS 103 301: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services".

## 2.2 Informative 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 referenced document (including any amendments) applies.

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

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] ETSI TR 102 638: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions".
- [i.2] ETSI TR 102 863: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM); Rationale for and guidance on standardization".
- [i.3] IEEE 1609.3™ 2010: "Wireless Access in Vehicular Environments (WAVE) - Networking Services".
- [i.4] CEN CEN/TS 16439: "Electronic fee collection - Security framework".
- [i.5] ETSI TS 102 890-2: "Intelligent Transport System (ITS); Facilities layer function; Part 2: Position and time facility specification".
- [i.6] IETF RFC 4949: Internet Security Glossary, Version 2, August 2007.
- [i.7] ETSI TS 102 723-8: "Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer".

---

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TS 102 731 [4], IETF RFC 4949 [i.6] and the following apply:

**identifier:** attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context

**security management:** operations that support acquiring or establishing the validity of certificates for cooperative ITS communications

### 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 302 665 [1], ETSI TS 103 301 [9] and the following apply:

AA	Authorization Authority
CA	Co-operative Awareness
CAM	Co-operative Awareness Message
CN	Co-operative Navigation
CRL	Certificate Revocation List
CS	Communities Services
CSM	Co-operative Speed Management
CSMS	Cooperative-ITS Security Management System
DENM	Decentralized Environment Notification Message
EA	Enrolment Authority
GN	GeoNetworking
HSM	Hardware Security Module

IP	Internet Protocol
IPv6	Internet Protocol version 6
ITS	Intelligent Transport System
ITS-S	ITS Station
LBS	Location Based Services
LCM	Life Cycle Management
MAC	Medium Access Control
OSI	Open System Interconnect
PDA	Personal Data Appliance
PKI	Public Key Infrastructure
RHW	Road Hazard Warning
RSU	Road Side Unit
SAP	Service Access Point
UML	Unified Modeling Language
WAVE	Wireless Access in Vehicular Environments
WSA	WAVE Service Announcement

## 4 ITS reference architecture

### 4.1 Background

ETSI EN 302 665 [1] describes an ITS station architecture based upon four processing layers identified as follows:

- Access Layer;
- Networking & Transport Layer;
- Facilities Layer; and
- Applications Layer.

These horizontal layers are bounded on each side by a vertical Management layer and a Security layer (figure 1).

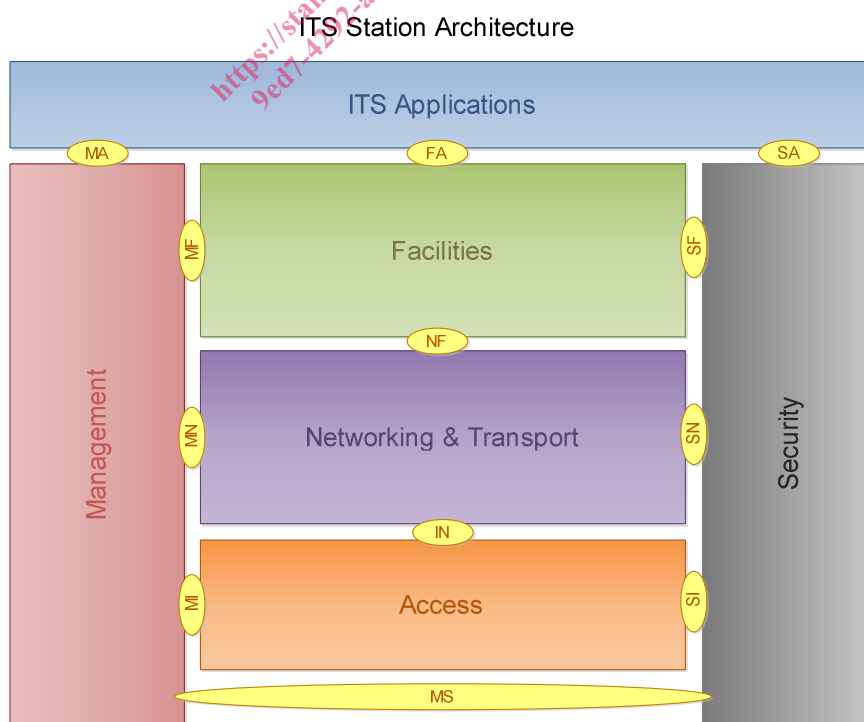
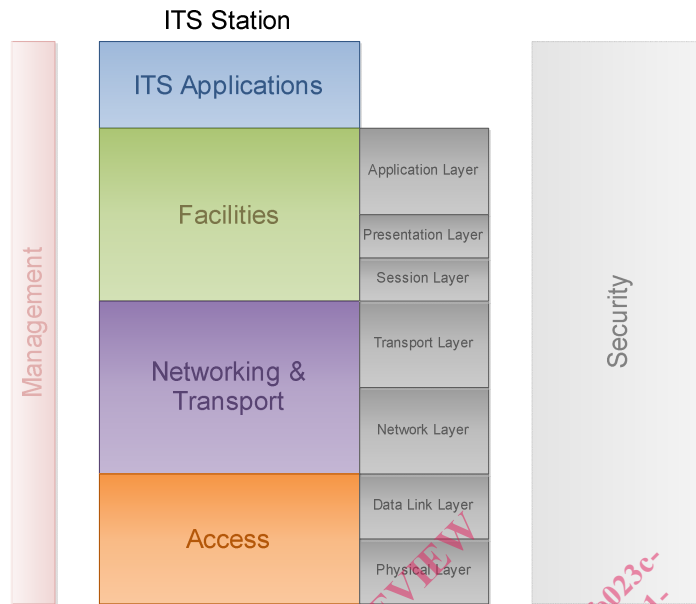


Figure 1: ITS station architecture (from ETSI EN 302 665 [1])

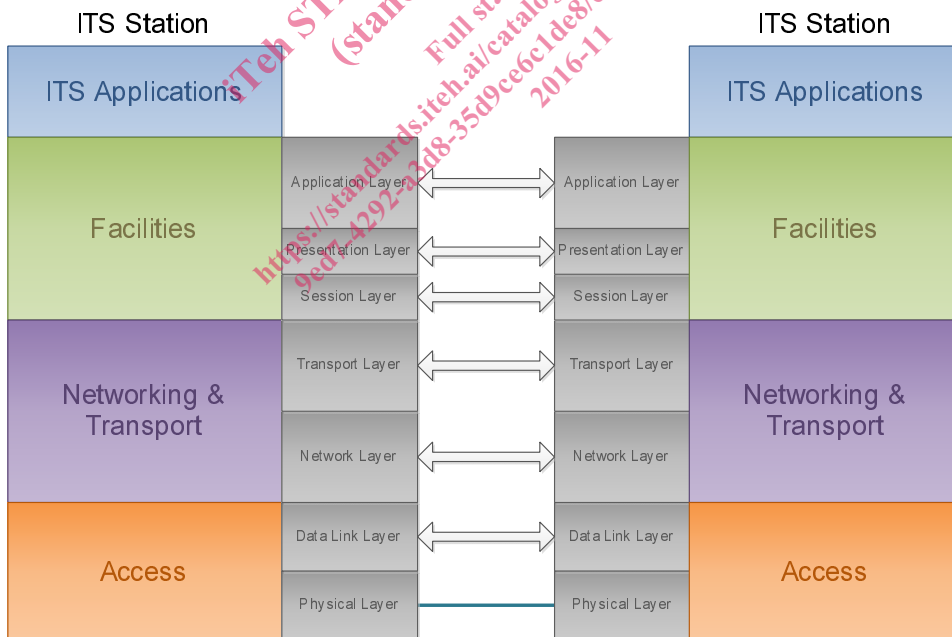


The layers in this architecture do not represent directly the Open System Interconnect (OSI) protocol modelling layers but the functionality expected in each can be mapped to OSI model quite simply (figure 2).



**Figure 2: Mapping of OSI modelling layers to the ITS architectural layers**

Having mapped the OSI protocol layers to the ITS station architecture, this can be extended into an ITS communications architecture in which the protocol layers communicate on a peer-to-peer basis as shown in figure 3.



**Figure 3: ITS communications architecture**

## 4.2 ITS applications groups

### 4.2.1 ITS applications groups and their communication characteristics

ETSI TR 102 638 [i.1] defines the basic set of ITS applications which it divides into groups according to the functionality provided. Based on this a further analysis in ETSI TR 102 863 [i.2] takes into account some additional sources. The resulting list of functional groupings from this analysis is shown in table 1. A more detailed description can be found in ETSI TR 102 863 [i.2], clause A.1.

**Table 1: ITS application classes**

Applications Class	Application	Use case
Active road safety	Driving assistance - Co-operative awareness (CA)	Emergency vehicle warning
		Slow vehicle indication
		Across traffic turn collision risk warning
		Merging Traffic Turn Collision Risk Warning
		Co-operative merging assistance
		Intersection collision warning
		Co-operative forward collision warning
	Driving assistance - Road Hazard Warning (RHW)	Lane Change Manoeuvre
		Emergency electronic brake lights
		Wrong way driving warning (infrastructure based)
		Stationary vehicle - accident
		Stationary vehicle - vehicle problem
		Traffic condition warning
		Signal violation warning
		Roadwork warning
		Decentralized floating car data - Hazardous location
		Decentralized floating car data - Precipitations
		Decentralized floating car data - Road adhesion
		Decentralized floating car data - Visibility
		Decentralized floating car data - Wind
Vulnerable road user Warning		
Pre-crash sensing warning		
Co-operative glare reduction		
Cooperative traffic efficiency	Co-operative speed management (CSM)	Regulatory/contextual speed limits notification
		Curve Warning
	Traffic light optimal speed advisory	
Co-operative navigation (CN)	Traffic information and recommended itinerary	
	Public transport information	
	In-vehicle signage	
Co-operative local services	Location based services (LBS)	Point of Interest notification
		Automatic access control and parking management
		ITS local electronic commerce
		Media downloading
Global internet services	Communities services (CS)	Insurance and financial services
		Fleet management
		Loading zone management
		Theft related services/After theft vehicle recovery
	ITS station life cycle management (LCM)	Vehicle software/data provisioning and update
		Vehicle and RSU data calibration
Transport related electronic financial transactions [i.4]		

In order to define security classes the communication patterns of the different applications also need to be considered. Table 2 summarizes the communication behaviour of each application.

**Table 2: ITS applications communication behaviour**

Use case	Addressing	Hops	Frequency	Direction	Session	
Emergency vehicle warning	Broadcast	Single	High	V2V/V2I	No	
Slow vehicle indication	Broadcast	Single	High	V2V	No	
Across traffic turn collision risk warning	Broadcast	Single	High	V2V	No	
Merging Traffic Turn Collision Risk Warning	Broadcast	Single	High	V2V/I2V	No	
Co-operative merging assistance	Broadcast	Single	High	V2V/I2V	No	
Intersection collision warning	Broadcast	Single	High	V2V/I2V	No	
Co-operative forward collision warning	Broadcast	Single	High	V2V	No	
Lane Change Manoeuvre	Broadcast	Single	High	V2V	No	
Emergency electronic brake lights	Broadcast	Multi	Low	V2V	No	
Wrong way driving warning (infrastructure based)	Broadcast	Single	Low	I2V	No	
Stationary vehicle - accident	Broadcast	Multi	Low	V2V/V2I	No	
Stationary vehicle - vehicle problem	Broadcast	Multi	Low	V2V/V2I	No	
Traffic condition warning	Broadcast	Multi	Low	V2V/I2V	No	
Signal violation warning	Broadcast	Single	High	I2V	No	
Roadwork warning	Broadcast	Multi	Low	I2V	No	
Decentralized floating car data - Hazardous location	Broadcast	Multi	Low	V2V/I2V	No	
Decentralized floating car data - Precipitations	Broadcast	Multi	Low	V2V	No	
Decentralized floating car data - Road adhesion	Broadcast	Multi	Low	V2V	No	
Decentralized floating car data - Visibility	Broadcast	Multi	Low	V2V	No	
Decentralized floating car data - Wind	Broadcast	Multi	Low	V2V	No	
Vulnerable road user Warning	Broadcast	Single	Low	V2V/I2V	No	
Pre-crash sensing warning	Indication	Broadcast	Single	High	V2V	No
	Data exchange	Unicast	Single	High	V2V	Yes
Co-operative glare reduction	Broadcast	Single	Low	V2V/I2V	No	
Regulatory/contextual speed limits notification	Broadcast	Single	Low	I2V	No	
Curve Warning	Broadcast	Single	Medium	I2V	No	
Traffic light optimal speed advisory	Broadcast	Multi	Medium	I2V	No	
Traffic information and recommended itinerary	Advertisement	Broadcast	Single	Low	I2V	Yes
	Service	Unicast/Multicast	Multi	Medium	I2V	No
Public transport information	Advertisement	Broadcast	Single	Low	I2V	No
	Service	Multicast	Multi	Medium	I2V	Yes
In-vehicle signage	Broadcast	Single	Medium	I2V	No	
Point of Interest notification	Advertisement	Broadcast	Single	Low	I2V	No
	Service	Multicast	Single	Low	I2V	Yes