ETSI TS 102 940 V1.3.1 (2018-04)

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

Reference
RTS/ITS-00541

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

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.

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".

[10] ETSI EN 302 636-4-1: "Intelligent Transport Systems (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".

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/TS 16439: "Electronic fee collection - Security framework".

[i.5] ETSI TS 102 890-2: "Intelligent Transport Systems (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".

[i.8] C-ITS Platform WG5: "Security & Certification Final Report ANNEX 1: Trust models for Cooperative - Intelligent Transport System (C-ITS)".

[i.9] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1, June 2017.

NOTE: Available at https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf.

3 Definitions, abbreviations and notation

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:

certificate revocation list (CRL): signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

certificate revocation list for authorities (CRL CA): certificate revocation list issued by a Root CA which contains only revoked certificates of the subordinate CAs within the hierarchical trust domain managed by the Root CA

certificate trust list: signed list indicating a set of trusted services of a PKI hierarchy controlled by a Root CA or a set of trusted Root CAs within the C-ITS Trust Domain controlled by a top-level authority (Trust List Manager)

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
C-ITS	Cooperative Intelligent Transport System
CN	Co-operative Navigation
CPOC	C-ITS Point Of Contact
CRL	Certificate Revocation List
CS	Communities Services
CSM	Co-operative Speed Management
CCMS	Cooperative-ITS security Certificate Management System
DENM	Decentralized Environment Notification Message
EA	Enrolment Authority
GN	GeoNetworking
HSM	Hardware Security Module
ID	Identity
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
MBD	MisBehaviour Detection
OSI	Open System Interconnect
PDA	Personal Data Appliance
PKI	Public Key Infrastructure
RHW	Road Hazard Warning
RSU	Road Side Unit
SAP	Service Access Point
TLM	Trust List Manager
UML	Unified Modeling Language
WAVE	Wireless Access in Vehicular Environments
WSA	WAVE Service Announcement

3.3 Notation

The requirements identified in the present document include:

a) mandatory requirements strictly to be followed in order to conform to the present document. Such requirements are indicated by clauses without any additional marking;

b) requirements strictly to be followed if applicable to the type of ITS Station concerned.

Such requirements are indicated by clauses marked by "[CONDITIONAL]"; and where relevant are marked by an identifier of the type of ITS-S for which the clauses are applicable as follows:

- [Itss_WithPrivacy] is used to denote requirements applicable to ITS-S for which pseudonymity has to be assured and re-identification by the AA is not allowed. This includes for instance personal user vehicle ITS-S or personal ITS-S Portable.

- [Itss_NoPrivacy] is used to denote requirements applicable to ITS-S for which pseudonymity does not have to be assured and are allowed to be re-identified by the AA. This may be for instance fixed or mobile RSUs or special vehicles.

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 entity and a Security entity (Figure 1).

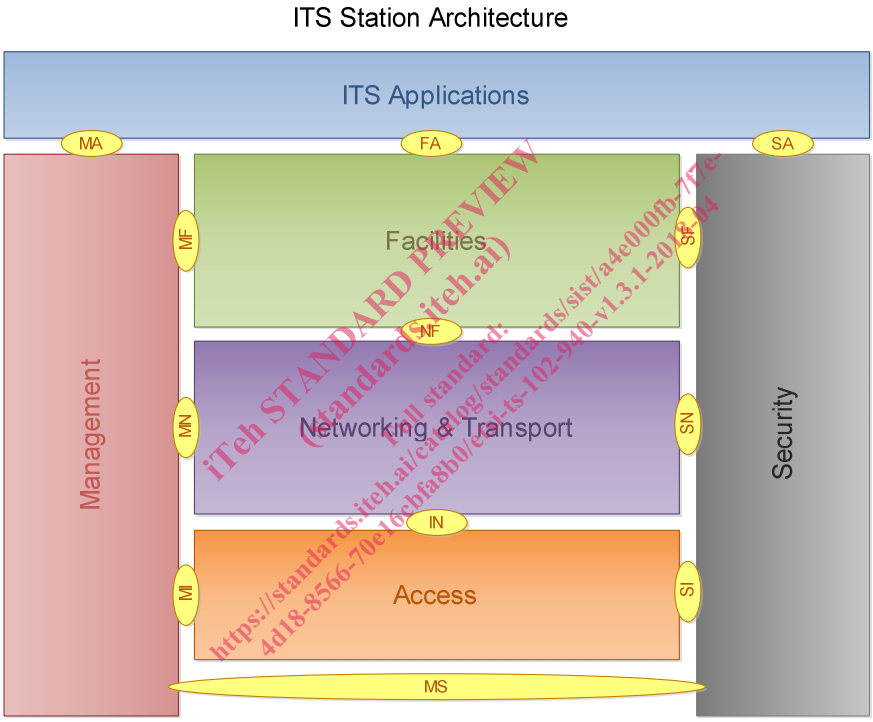

Figure 1: ITS station architecture (from ETSI EN 302 665 [1])

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. 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 2.

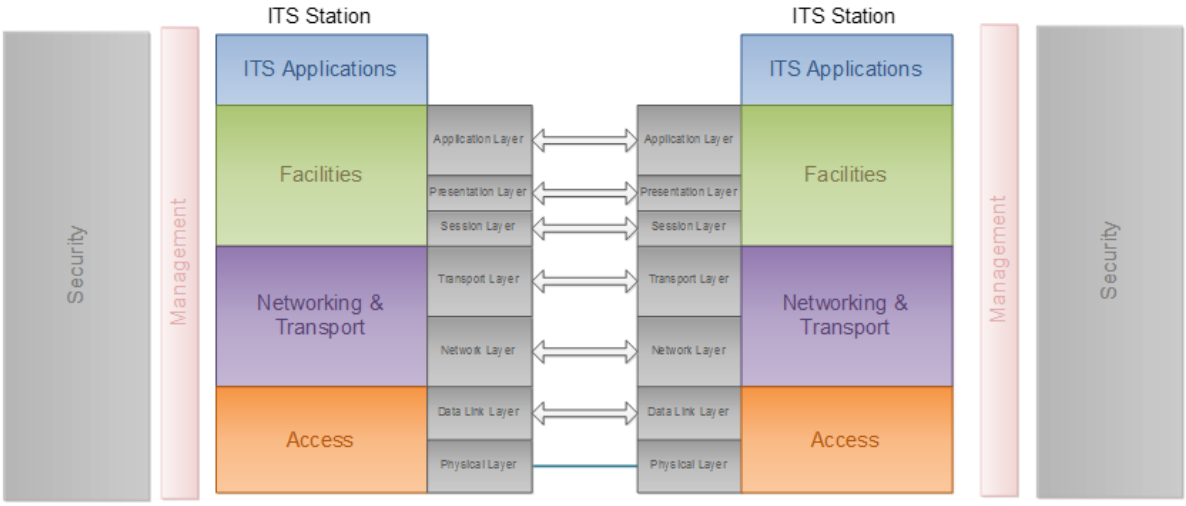

Figure 2: ITS communications architecture

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
		Lane Change Manoeuvre
	Driving assistance - Road Hazard Warning (RHW)	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	No
	Service	Unicast/Multicast	Multi	Medium	I2V	Yes
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