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

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).

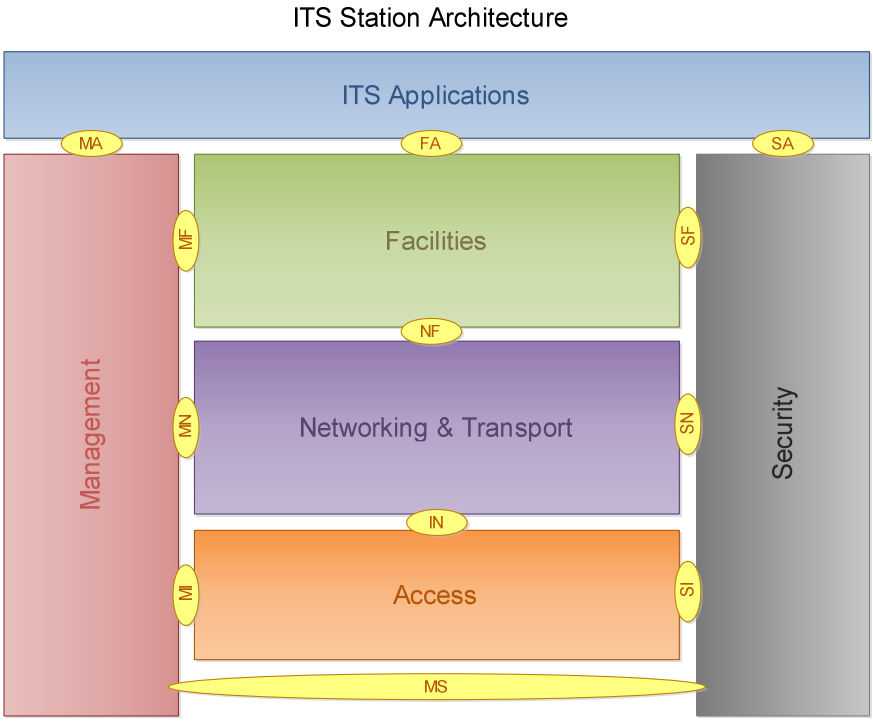


Figure 1: ITS station architecture (from ETSI EN 302 665 [1])

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.

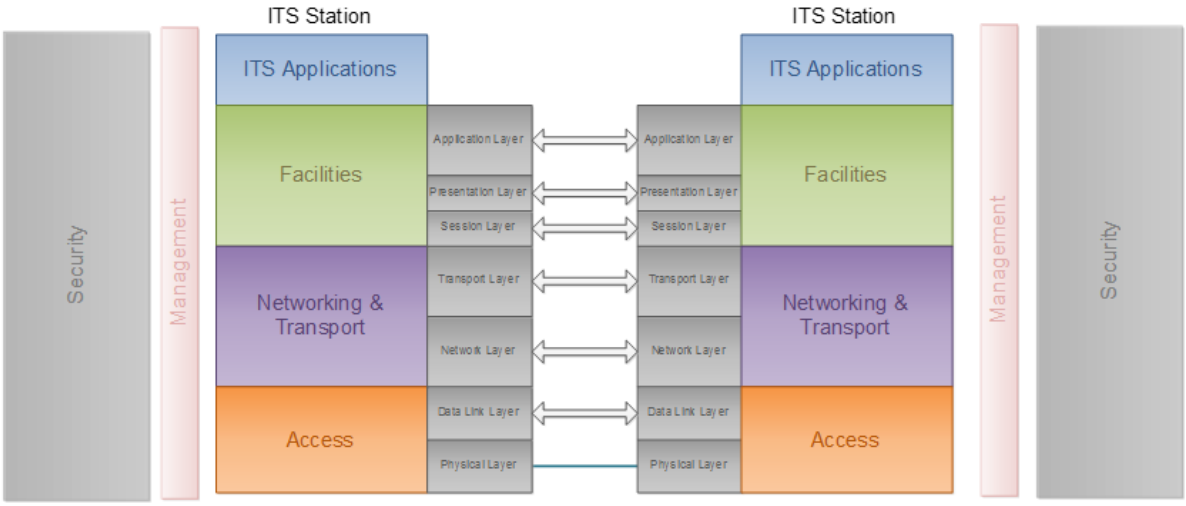


Figure 2: ITS communications architecture

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

Use case		Addressing	Hops	Frequency	Direction	Session
Automatic access control and parking management	Advertisement	Broadcast	Single	Low	I2V	No
	Service	Unicast	Single	Low	I2V/V2I	Yes
ITS local electronic commerce		Unicast	Single	Low	I2V/V2I	Yes
Media downloading		Unicast	Single	Low	I2V/V2I	Yes
Insurance and financial services		Unicast	Single	Low	I2V/V2I	Yes
Fleet management		Unicast	Single	Low	I2V/V2I	Yes
Loading zone management		Unicast/Multicast	Single	Low	I2V/V2I	Yes
Theft related services/After theft vehicle recovery		Unicast	Multi	Low	I2V/V2I	Yes
Vehicle software/data provisioning and update		Unicast	Single	Low	I2V/V2I	Yes
Vehicle and RSU data calibration		Unicast	Single	Low	I2V/V2I	Yes

The information in table 2 makes it possible to define a number of ITS application categories, thus:

- cooperative awareness;
- static local hazard warnings;
- interactive local hazard warnings;
- area hazard warnings;
- advertised services;
- local high-speed unicast services;
- local multicast services;
- low-speed unicast services; and
- distributed (networked) services.

These ITS application categories are further defined in clause 4.2.2 to clause 4.2.11.

4.2.2 Cooperative awareness

The purpose of cooperative awareness messages is to allow ITS users to provide other users with information regarding their status and environment in order to improve road safety. They can be categorized as follows:

- broadcast;
- single-hop;
- time-critical;
- having low data content;
- transmitted frequently;
- vehicle-to-vehicle;
- requiring no established communications session; and
- single message with no explicit coordination.

EXAMPLES: 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.

4.2.3 Static local hazard warning

Static local hazard warning messages are broadcast by fixed roadside ITS stations usually to provide continuous information regarding a specific static condition which is relevant to road users. They can be categorized as follows:

- broadcast only from a roadside ITS-S;
- single-hop;
- time-critical;
- having low data content;

- transmitted frequently;
- requiring no established communications session; and
- single message with no explicit coordination.

EXAMPLES: Merging traffic turn collision risk warning (if infrastructure-based),
Merging assistance (if infrastructure-based),
Intersection collision warning (if infrastructure-based),
Wrong way driving warning,
Signal violation warning.

Static local hazard warnings differ from cooperative awareness messages only in that they are transmitted by roadside ITS stations rather than vehicle-based stations. Consequently, they have different requirements for privacy preservation although all other security requirements are identical.

4.2.4 Interactive local hazard warning

Interactive local hazard warning messages are broadcast followed by a unicast session to provide direct cooperation in specific hazardous situations. The basic model for these applications is that station A receives a cooperative awareness message from station B and then returns a message to station B requesting that it takes a particular action. Based on this there may be additional data exchanges. These exchanges may contain more personal information than is included in cooperative awareness messages. They can be categorized as follows:

- broadcast followed by unicast;
- single-hop;
- time-critical;
- having low data content;
- transmitted frequently, but only if hazard exists;
- establish unicast communication session; and
- single message followed by coordinated session.

EXAMPLE: Pre-crash sensing warning.

4.2.5 Area hazard warning

Area hazard warning messages are broadcast and then forwarded by the receiving stations to form a geocast. They are sent event-driven to inform about a specific event or a specific condition to improve road safety. They can be categorized as follows:

- broadcast;
- multi-hop with geocasting;
- time-critical;
- low data content;
- transmitted frequently, but only when hazard exists;
- requires no established communication session.

EXAMPLES: Emergency electronic brake lights,
Stationary vehicle - accident,
Stationary vehicle - vehicle problem,
Traffic condition warning,
Roadwork warning,
Decentralized floating car data - hazardous location, precipitations, road adhesion, visibility, wind.

This category is also known as Decentralized Environmental Notification Messages (DENM) within ETSI.

Area hazard warnings are not sent regularly but only when a special situation or event occurred and are not always linked to a specific ITS-S as a point of origin. Thus, they cannot usually be used for tracking. Security mechanisms need to take into account the forwarding of the messages.

4.2.6 Advertised services

Advertised services refer to services where a provider unit sends out a message of a particular type advertising that the service is being offered and an ITS-S with the corresponding user application connects to the service. This description is based on WAVE Service Announcements (WSAs) as described in IEEE 1609.3 [i.3] but does not preclude any alternative method of providing Service Announcements including ETSI Facilities service announcement ETSI TS 102 890-2 [i.5].

Advertisements are not application messages themselves, though they may contain information allowing the user application to decide whether to connect. For example, a service advertisement for entertainment services might contain an identifier for the media provider.

They are broadcast as unencrypted messages and usually sent multiple times a second. They can be categorized as follows:

- broadcast by a service provider;
- single-hop;
- not time-critical;
- low data content;
- sent regularly to announce service;
- may be responded to in order to start a unicast session or enter a multicast session.

EXAMPLES: Public transport information (advertisement),
Traffic information and recommended itinerary (advertisement),
Point of interest notification (advertisement),
Automatic access control and parking management,
Media downloading (advertisement).

In many cases, the responding ITS-S will be associated with an end-user vehicle with a strong expectation of privacy.

4.2.7 Local high-speed unicast service

Local high-speed unicast services are provided directly to vehicles that may be moving at a high speed. They can be categorized as:

- unicast;
- single-hop;
- time critical;
- medium data content;
- frequently advertised then used as needed;
- local sessions.

EXAMPLE: Traffic information and recommended itinerary (service).

4.2.8 Local multicast service

Local multicast services are similar to local unicast service but using multicast communication. They can therefore be categorized as:

- multicast;
- single-hop;
- time critical;
- medium data content;
- frequently advertised then used as needed;
- local sessions.

EXAMPLES: Traffic information and recommended itinerary (service),
Public transport information (service),
Point of interest notification (service).

The distinguishing features of this type of service are that:

a) information is broadcast to the subscribers - it is in general non-interactive;

b) the service provider may want to provide the service to some but not all of the vehicles in a particular RSU's communication zone or in a particular larger region.

4.2.9 Low-speed unicast service

Low-speed unicast services are non time-critical services consumed at low (vehicle) speeds. They can be categorized as:

- unicast;
- single-hop;
- low time-criticality;
- medium to large data content;
- low frequency;
- restricted local or remote session.

EXAMPLES: ITS local electronic commerce,
Media downloading,
Insurance and financial services,
Fleet management,
Loading zone management,
Vehicle software/data provisioning and update,
Vehicle and RSU data calibration.

These services differ from high-speed unicast services in that the off-vehicle end of the communications session may be remote over the network. The application cannot rely on rapid exchange of large amounts of information and will have higher latency than the high-speed unicast service.

In general, these services will use an IP connection and so the use of existing IP security mechanisms may be appropriate.

NOTE: In general for ITS IP connections IPv6 will be used although the present document does not disallow any other variant of IP.

4.2.10 Distributed (networked) service

Distributed services are non-time critical subscription services that are intended to be consumed by the user over long periods such as the duration of a journey or even the lifetime of a vehicle. They can be categorized as:

- unicast;
- single-hop;
- low time-criticality;
- medium to large data content;
- low frequency;
- persistent remote session.

EXAMPLE: Real-time traffic information.

This service is similar to the low-speed unicast service in that it involves connecting with a service provider across a network. However, the difference is that the logical communication session needs to persist across multiple connections between the ITS-S and the roadside infrastructure. The persistence may be provided at the application level, the transport layer, or the internet layer.

4.2.11 Multiple Applications

An ITS-S may run multiple applications. Each application will have its own security requirements as described above. However, the combination of applications may introduce additional threats to the communications security, such as:

- Privacy - the combination of applications that an ITS-S runs may act as an identifier.
- Availability - one application may consume resources needed by another application.

These issues are mainly handled by mechanisms in the ITS-S before messages are transmitted (see clause 6).

4.3 Security requirements of ITS application groups

4.3.1 Security requirements of cooperative awareness

4.3.1.1 Authentication and Authorization

Cooperative awareness applications are used to enhance traffic safety. In addition to authenticity and integrity, authorization is required in order to restrict access to legitimate users. Different levels of authentication may be needed depending on the application and the requirements for participation. Consequently, authorization may depend on status (e.g. vehicle priority), properties (e.g. sensor equipment, implementation, vehicle type) or subscription to a chargeable service (e.g. personalized route guidance).

In general, authentication is required for applications that intend to send messages over the network. Thus, for CAM this may be a central service (on the ITS-S) that may be called by the single applications.

There are several classes of CAM authorization:

- Basic CAM authorization:
  - linked to basic data such as length, width, speed, heading, acceleration and brake status;
  - granted to all enrolled ITS stations to enable participation in the basic ITS.
- Advanced CAM authorization:
  - contains additional information such as that required for across traffic turning, merging assistance and collision warning;

  - depends on the abilities of the sending station such as the cryptographic algorithms implemented, its sensors and its perceived trustworthiness.

- Authorization to claim priority rights for emergency vehicles:
  - granted only to specially authorized emergency vehicles or public transport vehicles according to national legislation. Multiple layers of priority may be defined, for example priority for emergency vehicles and on a lower level authorization to use a special lane reserved for public transportation;
  - granted by a governmental organization or its authorized proxy agency;
  - priority rights asserted by the user during operation, not during authorization.
- Authorization to state regulatory orders such as speed limits and road closures:
  - granted only to specially authorized ITS stations such as RSUs and police vehicles;
  - granted by a governmental organization or its authorized proxy agency.

4.3.1.2 Confidentiality

As CAMs are broadcasts to any possible receiver there are no confidentiality requirements.

4.3.1.3 Privacy

CAMs are sent periodically up to several times a second by every ITS-S. They contain substantial status information (e.g. location) relating to the sending ITS-S. Consequently, it is necessary to ensure that the data cannot be linked to any individual so that no personally identifying information is leaked by the CAM service. Details to security mechanisms and policies provided to protect privacy are given in ETSI TS 102 941 [5].

4.3.2 Security requirements of static local hazard warnings

4.3.2.1 Authentication and Authorization

Static local hazard warnings have very similar properties than the CAM service with the exemption that they are sent by RSUs. For Authentication and Authorization similar requirements as for CAM apply with the addition, that authorization should be limited to the specific purpose, functionality, and location of the respective RSU.

4.3.2.2 Confidentiality and Privacy

As the nature of the service is broadcast and the sender is a static RSU, no confidentiality or privacy requirements apply.

4.3.3 Security requirements of interactive local hazard warnings

4.3.3.1 Authentication and Authorization

In general the requirements for Authorization and Authentication are similar to CAM. In the subsequent unicast session the local policies of the participating partners may require additional authorization and/or authentication. These additional requirements are out of the scope of the present document.

4.3.3.2 Confidentiality and Privacy

The requirements for Confidentiality and Privacy depend heavily on the specific application and the information to be exchanged. The unicast session may contain more privacy related and personally identifying information so that confidentiality may be an issue but this is likely to be solved within the application or bilaterally between involved parties. These requirements are, thus, out of scope of the present document.

4.3.4 Security requirements of area hazard warnings

4.3.4.1 Authentication and Authorization

Authorization for area hazard warnings (Decentralized Environment Notification Message, DENM) could be granted on several levels depending on sensor equipment, sensor quality and algorithmic and processing capabilities of the ITS-S. Apart from that, similar requirements as for CAM apply.

4.3.4.2 Confidentiality and Privacy

As the service is event-driven and, therefore, sporadic and as neither the properties of the sender nor its identity are important for the reported area warning, the privacy issues are reduced compared with the CAM service. Consequently, no confidentiality services are required.

4.3.5 Security requirements of advertised services

4.3.5.1 Authentication and Authorization

The Service Advertisement Message (SAM/WSA) is used by a service provider unit to inform ITS stations about available local services or about services that can be accessed on a remote server.

To minimize the risk of threats to ITS stations such as attacks from a fake or malicious service provider unit or an impersonation of an Internet server, the Service Advertisement message shall be protected for integrity and authenticity: such message shall be signed by the ITS-S (road-side or vehicle) providing the service advertisement to its neighbour ITS-S.

In general, authentication is required for applications that intend to send messages over the network. In addition special authorization shall be granted to the ITS-S for the purpose of this specific service advertisement application.

4.3.5.2 Confidentiality and Privacy

As the nature of service is broadcast to any possible receivers and the sender is a static RSU or a mobile vehicle which accepts to play a distinguishable role (e.g. leader vehicle in a platoon), no confidentiality or privacy requirements apply.

4.3.6 Security requirements of other services

Special authorization may be needed for commercial services. The authorization model depends on the specific service provided and the local legal conditions which may vary between countries. Authorization may include fees. Local services such as multimedia download may need confidentiality in addition depending on the copyright of the contents and the business model of the service.

In general, security requirements depend heavily on the type and the business model of the service. These specific requirements are out of the scope of the present document.

4.3.7 Security requirements of multiple applications

4.3.7.1 Authentication and Authorization

In general, Authentication and Authorization are handled separately for each individual application. Nevertheless, some combinations of applications may require special treatment or authorization due to additional privacy issues. This needs to be dealt within security policies associated with the authorization or during the authorization process itself.

4.3.7.2 Confidentiality and Privacy

It is assumed that each ITS application uses its own identifiers that cannot be linked to each other. In particular, DENM and CAM originating from the same vehicle should not be linkable.

5 ITS communications security architecture

5.1 ITS station communications security architecture

ETSI EN 302 665 [1] shows Security as a vertical layer adjacent to each of the ITS layers but, in fact, security services are provided on a layer-by-layer basis so that the security layer can be considered to be subdivided into the four basic ITS processing layers as shown in Figure 3.

Security services are provided on a layer-by-layer basis, in the manner that each of the security services operates within one or several ITS architectural layers, or within the Security Management layer.

Figure 3 shows the security services and Security Management functional entities.

Furthermore, the Security Entity of the ITS communications architecture as specified in ETSI EN 302 665 [1] provides a third sublayer: the security defense layer of the communicating ITS-S, which prevents direct attacks against critical system assets and data and increases the likelihood of the attacker being detected (e.g. Firewall and Intrusion detection or prevention). This latest sublayer is out of scope of the present document.

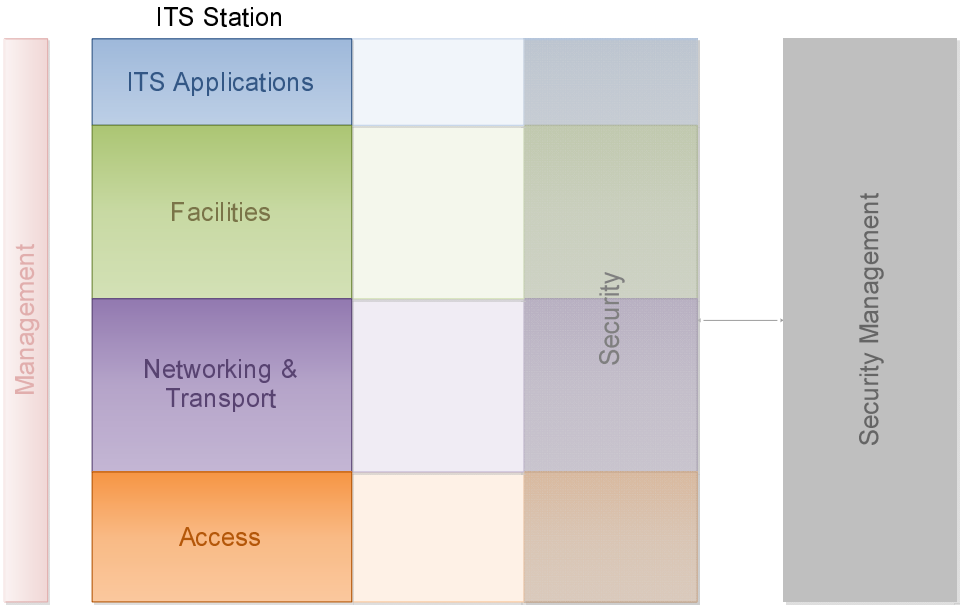


Figure 3: Architectural ITS security layers

Figure 4 shows the functional entities of the ITS-S communications security architecture and the relationship that exist between themselves and the ITS-S communication layers (SF-SAP, SN-SAP, and SI-SAP specified in ETSI EN 302 665 [1]).

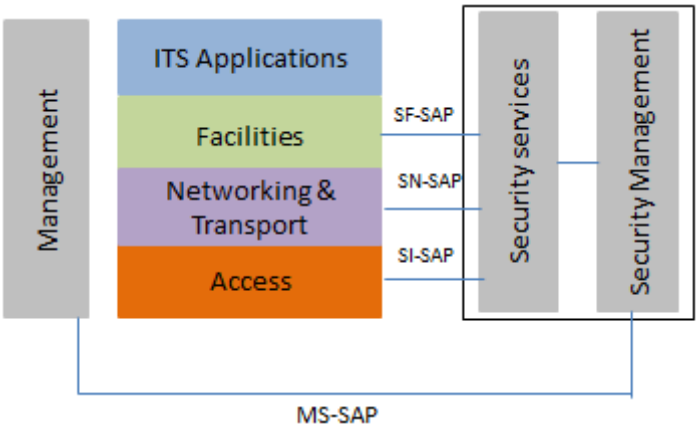


Figure 4: ITS-S security architecture: entities and interfaces

NOTE: The ITS-S security defence layer is not shown in Figure 4.

5.2 Security services

ETSI TS 102 731 [4] identifies a range of security services which may be supported by an ITS station in order to provide communications security between itself and other stations. Table 3 provides the list and a short description of these services.

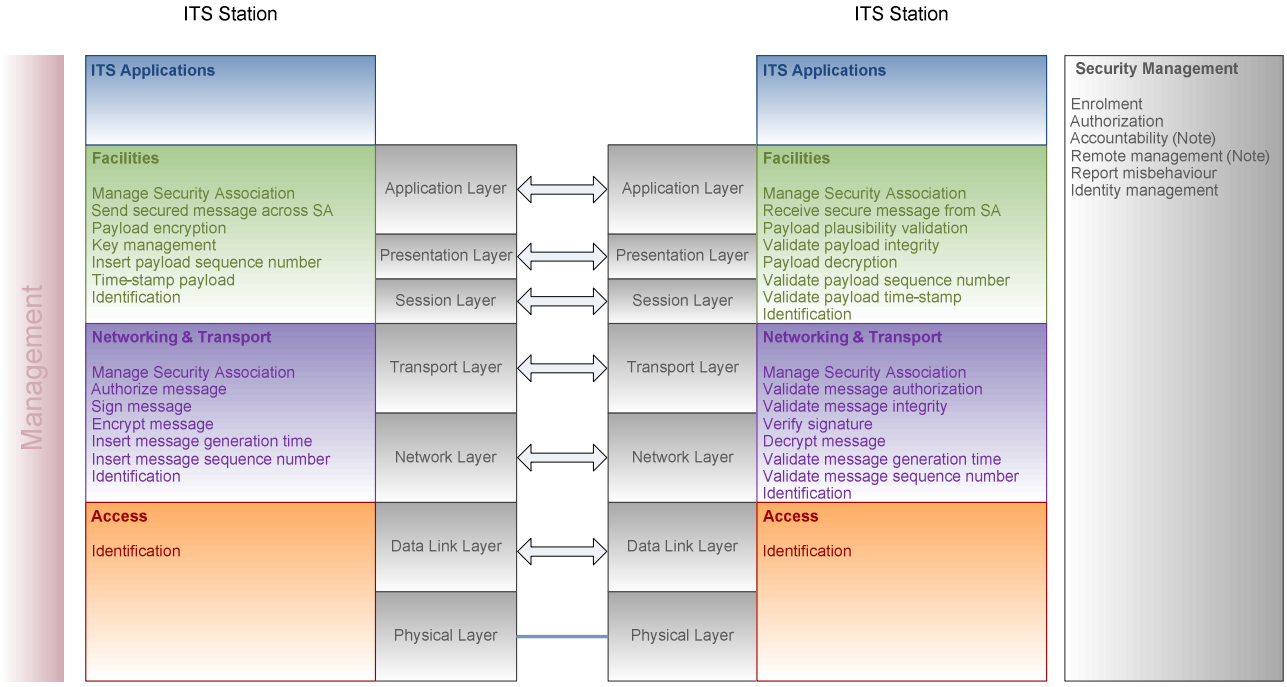
Table 3: ITS Communication Security Services

Service category	Security service	Short description
Security Associations management	Establish Security Association	Establishment of a secure communication between two ITS stations such that they can exchange messages securely. In order to establish a bi-directional secure communication both ITS station shall invoke this service.
	Update security association	
	Send Secured Message	
	Receive Secured Message	
	Remove security association	
Single message services	Authorize Single Message	This service secures the sending or receiving of a single message (like a CAM or DENM).
	Validate Authorization on Single Message	
	Encrypt Single Message	
	Decrypt Single Message	
Integrity services	Calculate Check Value	Calculation of a check value for inclusion into an outgoing message. Verification that an incoming message has not been altered (using its check value).
	Validate Check Value	
	Insert Check Value	
Replay Protection services	Replay Protection Based on Timestamp	Verification that messages are sent/received in a consistent manner by including a timestamp/sequence number in outgoing messages and by checking the timestamp/sequence number of incoming messages.
	Replay Protection Based on Sequence Number	
Plausibility validation	Validate Data Plausibility	Verification that information extracted from an incoming message can be trusted on the basis of its plausibility.

Table 4: ITS Communication Security Management Services

Service category	Security service	Short description
Enrolment	Obtain Enrolment Credentials	Management of enrolment credentials. An ITS station shall request enrolments credentials to an Enrolment Authority such that it can be trusted to function correctly by other ITS stations.
	Update Enrolment Credentials	
	Remove Enrolment Credentials	
Authorization	Obtain Authorization Tickets	Management of authorization tickets. An enrolled ITS station shall request authorization tickets to an Authorization Authority to get specific permissions (e.g. to access to a specific service/resource).
	Update Authorization Tickets	
	Publish Authorization Status	
	Update Local Authorization Status Repository	
Accountability services	Record Incoming Message in Audit Log	Records incoming/outgoing messages such that the ITS station can be held accountable.
	Record outgoing message in Audit Log	
Remote management	Remote Activate Transmission	Enable the ITS infrastructure to remotely manage a misbehaving ITS station. More precisely, this service enables the ITS infrastructure to remotely activate or deactivate the transmission of messages on a specific ITS station.
	Deactivate ITS transmission	
Report Misbehaving ITS-S	Report misbehaviour	Enable ITS stations to report a suspicious activity to the ITS infrastructure (e.g. a misbehaving ITS station).
Identity Management	Subscribe ID Change Notification	Provide services supporting the simultaneous change of communication identifiers (like station ID, network ID, MAC address) and credentials used for secure communications, within the ITS station. Provides features allowing the disabling of ID change.
	Unsubscribe ID Change Notification	
	ID Change Notification	
	Trigger ID Change	
	Lock ID Change	
	Unlock ID Change	

Each of the services summarized in table 3 operates within one or more of the ITS architectural layers and each of the services summarized in table 4 operates within the Security Management layer as shown in Figure 5.



NOTE: Figure 5 is based on ETSI TS 102 731 [4] security services. The Accountability and Remote management security management services are not specified in the present document.

Figure 5: The placement of security services within the ITS station architecture

5.3 ITS security functional model

Communications security services require, by definition, more than one element within their functional model. The principle functional elements and reference points between them can be determined by considering a simple ITS communications scenario such as that shown in Figure 6. This shows an ITS-enabled vehicle which needs to communicate with the following entities:

- an enrolment authority;
- an authorization authority;
- other ITS-equipped vehicles; and
- other ITS-equipped devices:
  - roadside units; and
  - personal units such as portable devices.

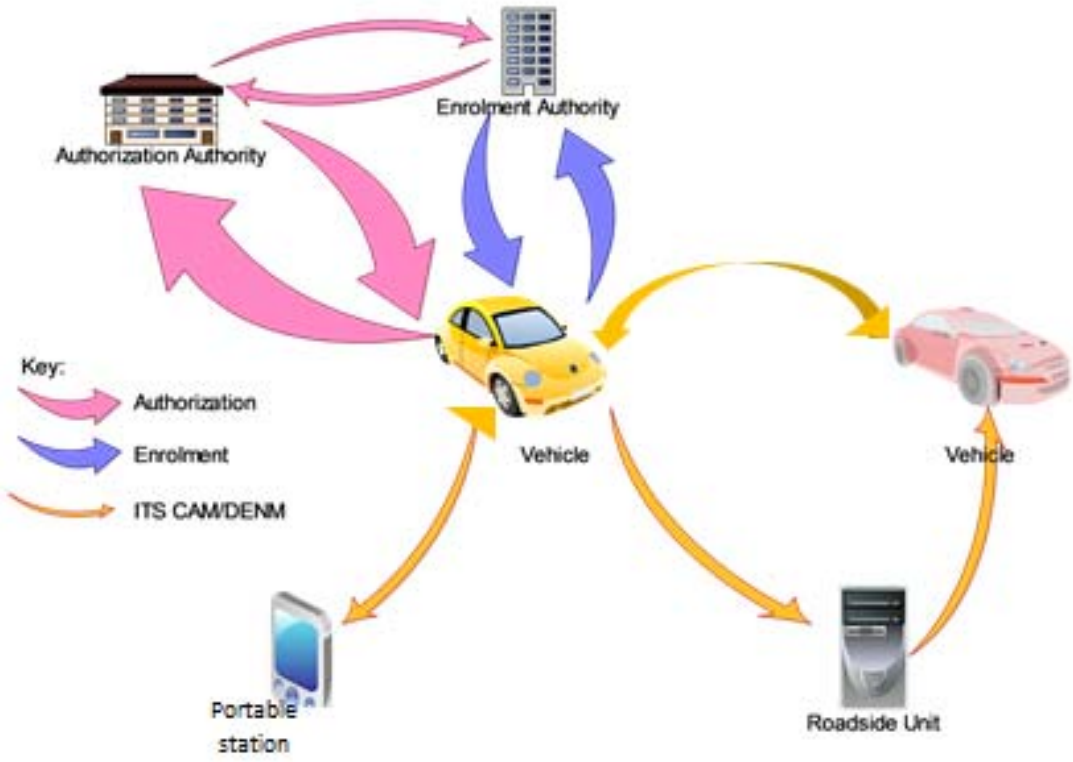


Figure 6: ITS communications reference scenario

The reference configuration implied by this scenario requires functional elements to represent each of the entities shown in Figure 6. These elements and the reference points between them are identified in Figure 7.

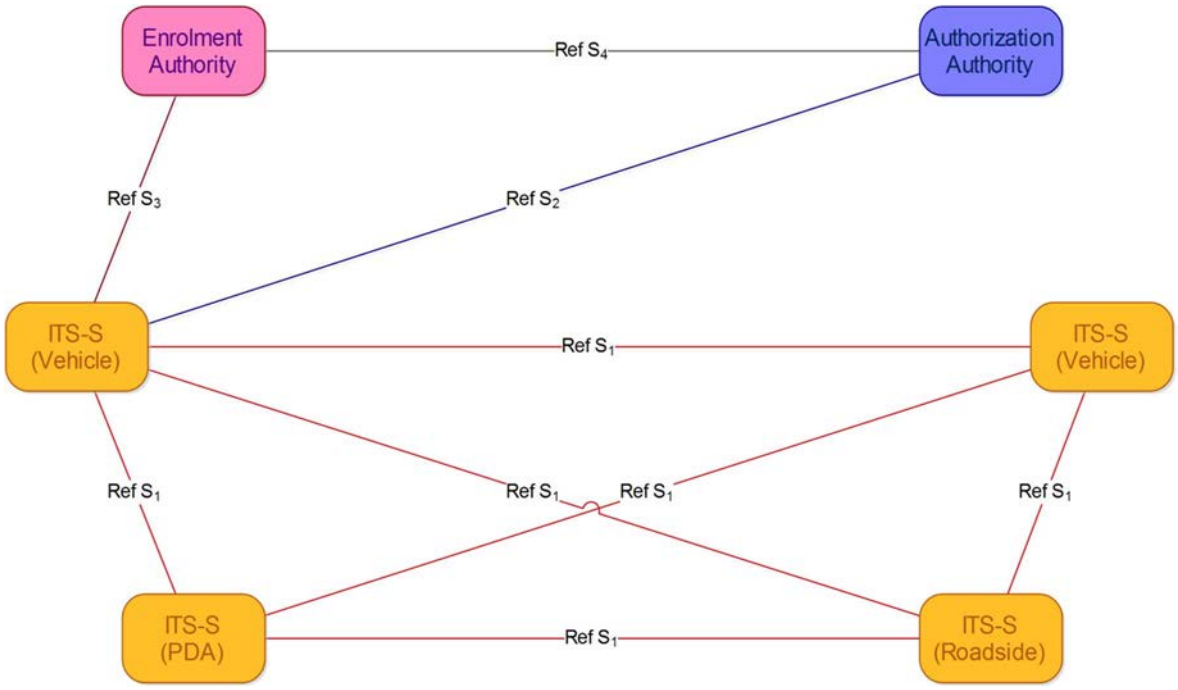


Figure 7: ITS security functional elements and reference points

NOTE 1: The naming of the reference points in this model as S_1 to S_4 is arbitrary and introduced purely for ease of describing the model. The nomenclature may be changed later on when standardized ITS reference points are defined.

NOTE 2: Reference points S_2 and S_3 exist between each ITS-S and the Authorization Authority and the Enrolment Authority respectively. For the purposes of clarity, they have been omitted from the diagram in Figure 7.

This model can be further refined by considering each of the ITS Stations (ITS-S) to be functionally identical regardless of the hosting equipment (vehicle, roadside unit or PDA) with one ITS-S representing the station sending a message and another one representing the message recipient. The resultant ITS security reference model (Figure 8) can be used as the basis for specifying all ITS security services related to single-hop broadcast services such as CAM. However, a different model involving a third ITS-S for relaying messages needs to be considered for all ITS security services associated with relayed, broadcast services such as DENM (Figure 9).

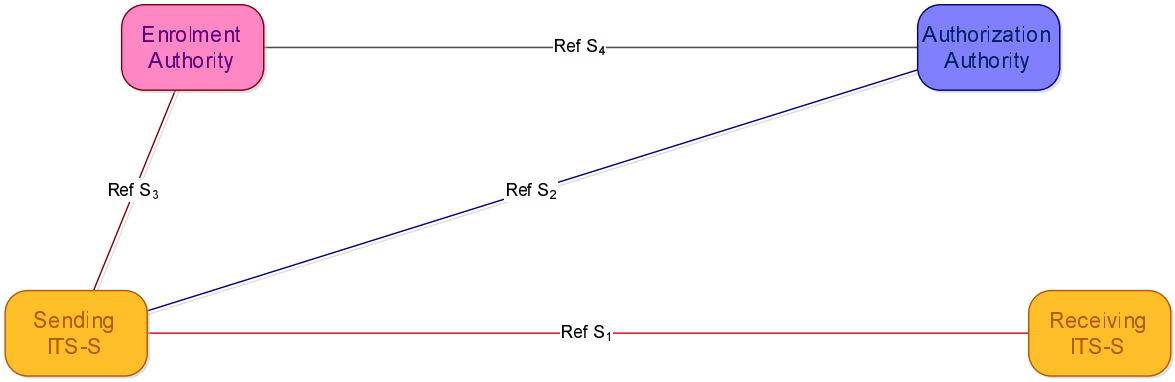


Figure 8: ITS security reference model for CAM

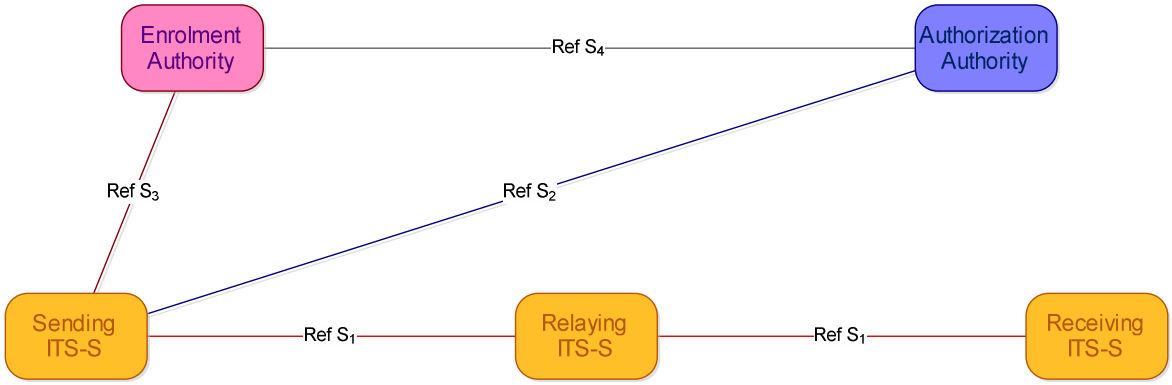


Figure 9: ITS security reference model for DENM

Each of the functional elements in the ITS security reference models has a specific role to play and these are summarized in table 5.

Table 5: Functional element roles

Functional element	Role
Enrolment Authority	Authenticates an ITS-S and grants it access to ITS communications
Authorization Authority	Provides an ITS-S with authoritative proof that it may use specific ITS services
Sending ITS-S	Acquires rights to access ITS communications from Enrolment Authority Negotiates rights to invoke ITS services from Authorization Authority Sends single-hop and relayed broadcast messages
Relaying ITS-S	Receives broadcast message from the sending ITS-S and forwards them to the receiving ITS-S if required
Receiving ITS-S	Receives broadcast messages from the sending or relaying ITS-S

Information is exchanged between the functional elements in the ITS security reference model across four defined reference points identified as S_1, S_2, S_3 and S_4. The characteristics of each of these reference points are summarized in table 6.

Table 6: Summary of ITS security reference points

Reference Point	Functional Element		Information carried
	From	To	
S_1	Sending ITS-S	Receiving ITS-S	Message payload such as: CAM defined in ETSI EN 302 637-2 [2], SPATEM defined in ETSI TS 103 301 [9], MAPEM defined in ETSI TS 103 301 [9], IVIM defined in ETSI TS 103 301 [9], SREM defined in ETSI TS 103 301 [9], SSEM defined in ETSI TS 103 301 [9].
	Sending ITS-S	Relaying ITS-S	Message payload such as: DENM defined in ETSI EN 302 637-3 [3], SPATEM defined in ETSI TS 103 301 [9], MAPEM defined in ETSI TS 103 301 [9], IVIM defined in ETSI TS 103 301 [9], SREM defined in ETSI TS 103 301 [9], SSEM defined in ETSI TS 103 301 [9].
	Relaying ITS-S	Receiving ITS-S	Message payload such as: DENM defined in ETSI EN 302 637-3 [3], SPATEM defined in ETSI TS 103 301 [9], MAPEM defined in ETSI TS 103 301 [9], IVIM defined in ETSI TS 103 301 [9], SREM defined in ETSI TS 103 301 [9], SSEM defined in ETSI TS 103 301 [9].
S_2	Sending ITS-S	Authorization Authority	Requests for authorization to invoke ITS security services, see ETSI TS 102 731 [4].
	Authorization Authority	Sending ITS-S	Authorization parameters, see ETSI TS 102 731 [4].
S_3	Sending ITS-S	Enrolment Authority	Request for permission to access ITS communications, see ETSI TS 102 731 [4].
	Enrolment Authority	Sending ITS-S	Enrolment credentials, see ETSI TS 102 731 [4].
S_4	Authorization Authority	Enrolment Authority	Request for verification of ITS-S enrolment credentials, see ETSI TS 102 731 [4].
	Enrolment Authority	Authorization Authority	Verification of ITS-S enrolment credentials, see ETSI TS 102 731 [4].

The information passing across each ITS security reference point supports a range of the communications security services specified in table 3 and table 4. The distribution of security services to the reference points is specified in table 7.

NOTE 3: Table 7 specifies the security services provided on the reference points S_1, S_2, S_3 and S_4 and the list of services provided at the internal interface between ITS-S security entity and other ITS-S architecture entities (SF-SAP, SN-SAP and SI-SAP) defined in ETSI EN 302 665 [1].

Table 7: Communications security services supported at ITS security reference points

Reference point	Security services supported
S_1	Establish Security Association
	Update Security Association
	Send secured message
	Receive secured message
	Remove Security Association
	Confidentiality services
	Integrity services
	Replay protection services
S_2	Obtain authorization tickets
	Update authorization tickets
	Publish authorization status
	Update local authorization status repository
	Report misbehaving ITS-S
S_3	Obtain enrolment credentials
	Update enrolment credentials
	Remove enrolment credentials
	Remote activate ITS transmission
	Remote deactivate ITS transmission
	Report misbehaving ITS-S
S_4	Obtain authorization tickets
	Update authorization tickets
	Publish authorization status
	Update local authorization status repository
Internal - confidentiality (see note)	Authorize single message
	Validate authorization on single message
	Encrypt single message
	Decrypt single message
Internal - Integrity (see note)	Calculate check value
	Insert check value
	Validate check value
	Validate data plausibility
Internal - replay protection (see note)	Time-stamp message
	Sequence number message
Internal - accountability (see note)	Record incoming message in audit log
	Record outgoing message in audit log
Internal - Identity Management (see note)	Lock ID Change
	Unlock ID Change
	Subscribe ID change Notification
	Unsubscribe ID change Notification
	ID Change Notification
	Trigger ID Change
NOTE: These services are required to support ITS communications security services but do not involve the exchange of information across one of the reference points.	

6 ITS station security management

6.1 Basic principles

The purpose of the present document is to describe an architecture for the communication security of ITS. However, it is also necessary for an ITS-S to provide secure access to common resources such as services, information and protocols. These security requirements can be separated into two parts:

1) external security:

   - security related to the behaviour of the ITS-S as a communication endpoint:

     - security and trust towards the external communication peer;

        - security and trust towards the network;

2) internal security:

    - security related to the ITS-S as a processing platform and application host:

        - protection of applications from the actions of other applications;
        - protection of shared information;
        - protection of shared processing resources such as communications software and hardware.

The ITS communication system relies on indirect trust relationships built statically using certification by trusted third parties (TTPs), mainly the enrolment authority (EA). Enrolment is the main access control to the ITS and the possession of a valid enrolment certificate grants permission to the station to be part of the ITS and, subsequently, to gain authorization for the use of further services. It should, therefore, be restricted to stations that fulfil a set of security properties that are considered to make the platform trusted (clause 6.2). The basic requirements and procedures for enrolment are specified in more detail in ETSI TS 102 941 [5].

6.2 Guidelines for establishing enrolment trust requirements

The following recommendations are specified as guidance in ensuring that an ITS-S is able to establish a trust relationship with an enrolment authority:

- all cryptographic key material should be stored in a secure memory that is protected against tampering, altering and unauthorized reading and should only be accessible over a clearly defined, secure interface using appropriate means for authentication and authorization;
- access to key material should only be possible for authorized entities within the ITS-S and bound to a trusted, uncompromised system state;
- keys should be communicated in an encrypted form rather than in plaintext;
- keys should only be communicated to a secure processing engine (referred to as a cryptographic module);
- modules and applications other than the cryptographic module should have access only to key handles;
- a cryptographic module and its interface to the storage should be protected against tampering, eavesdropping, manipulation and other forms of attack;

Key storage and cryptographic functions should be integrated into a secure module, preferably in tamper resistant hardware, protecting the key material and offering cryptographic operations as services to all other applications and security services within the constraints of an appropriate authorization mechanism. This secure module is named Hardware Security Module (HSM). Figure 10 shows, in generic terms, how this could be structured.

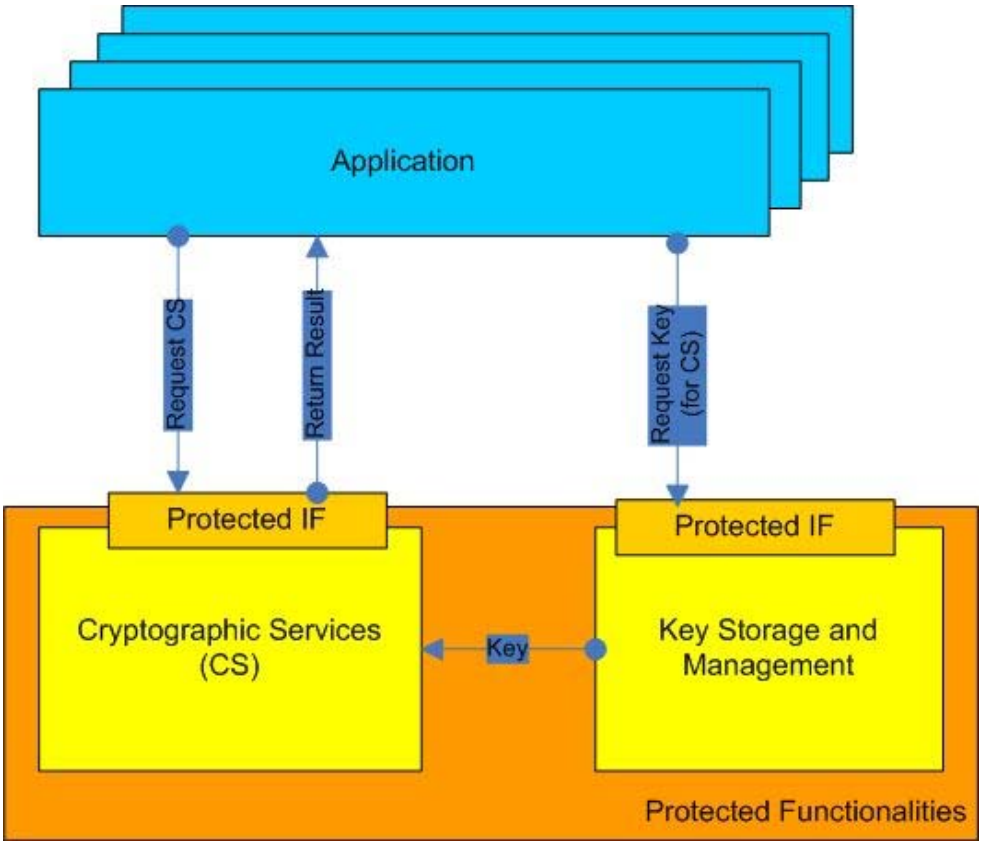


Figure 10: Abstracted generic model of a Hardware Security Module (HSM) for ITS-S security

- applications should be securely separated to avoid unsolicited interaction;
- access to ITS keys and other sensitive data by applications should require explicit authorization and be managed over a clearly defined, protected interface.

6.3 Trust and privacy management

The enrolment and authorization services (table 4) provide the following services to support the establishment of trust and the protection of privacy:

- trust:
  - the provision of certificates allowing an ITS station to assert:
    - their permission to use the ITS system as a whole; and
    - their permission to use specific ITS services and applications;
- privacy:
  - the provision of pseudonyms that can be used in place of a more meaningful (and traceable) identifier and that can be changed frequently to avoid simple correlation between the pseudonym and the vehicle (or person) with which it is associated.

The procedures and protocol required by the enrolment and authorization services are specified in detail in ETSI TS 102 941 [5].

6.4 Access control

Before an ITS station can make full use of the ITS applications, services and capabilities that are available to it, it is required to obtain specific credentials from the Authorization Authority. These credentials, in the form of cryptographically signed certificates, are used to assure any receiving ITS-S that the station has the necessary permission to send the particular service-specific information and that it can be trusted.

Authorization tickets are only issued to an ITS-S after a comprehensive procedure has been followed in order to protect its identity and avoid misuse of ITS services and capabilities. This procedure involves:

- Initialization:
  - performed in conjunction with the manufacturer of the vehicle or ITS device;
  - establishes a set of initialization credentials:
    - a canonical (unique and immutable) identity for the ITS-S;
    - a canonical public and private cryptographic key pair for the ITS-S;
    - a generic profile of the properties of the ITS-S (for example, the proven stability of its software and hardware, its resistance to attack and the ITS facilities that it is able to support);
    - optionally, a cryptographic certificate (self-signed bootstrap certificate) linking the canonical identity with the public key of the ITS-S and its generic profile.
- Enrolment:
  - performed as a dialogue between the ITS-S and the Enrolment Authority;
  - uses the canonical credentials to establish a set of enrolment credentials at initialization and then the previously issued enrolment credentials to renew the enrolment credentials:
    - one or more cryptographic certificates indicating the applications, services and capabilities that the ITS-S is permitted to use and which enable the ITS-S to pseudonymously request authorization from the Authorization Authority to invoke those services.
- Authorization:
  - performed as a dialogue between the ITS-S and the Authorization Authority;
  - uses the enrolment credentials to establish a set of authorization credentials:
    - one or more cryptographically signed authorization ticket which, when combined with a transmitted ITS message, enables the ITS-S to assert pseudonymously to other ITS stations its right to send that particular message or information.

The detailed requirements of this access control procedure are specified in ETSI TS 102 942 [6] and the protocols required to support it can be found in ETSI TS 102 941 [5].

6.5 Identity management

The present document defines a set of requirements for ITS-S of different categories. Using the notation defined in clause 3.3, the set of requirements that are applicable for privacy protection are labelled with [Itss_WithPrivacy].

The Authorization Authority provides an ITS station with multiple authorization tickets (or pseudonym certificates) to be used in the ITS communication over its life time. The authorization ticket pseudonymises the ITS-S identity whilst in the same time proving it is authenticated and authorized to access communication resources and services.

[Itss_WithPrivacy] the ITS-S shall provide a mechanism for changing frequently the ITS-S pseudonym certificate.

Identity management including credential creation, storage, certification and revocation is provided internally by the Security Entity, as part of Security Management as shown in Figure 4.

Security services covering the use and change of identification information within an ITS station is shown in table 4.

Use of security credentials is opaque to the calling ITS communication layer, except for the changing of identification information in the ITS communication Layers (ID Change service shown in table 4). The ID Change service execution is coordinated by the Security Management and relies at each communication layer on the 'identification' function as shown in Figure 5.

Changing authorization tickets in the communication stack may only provide unlinkable pseudonymity, if all identifiers are changed at the same time.

[Itss_WithPrivacy] Therefore, all the IDs associated with the ITS-S across different layers of the communication stack shall be changed synchronously with the Authorization Ticket: this requires that the Security Entity communicates the certificate identifier each time it is changing of authorization ticket. The information used to identify an ITS-S certificate is the *HashedID8* of the certificate as specified in ETSI TS 103 097 [8].

[Itss_WithPrivacy] the ITS station shall apply the following requirements when changing of pseudonym certificate (AT):

- All the IDs associated with a node across different layers of the ITS stack shall be changed synchronously using the ID Change Notification service as shown in table 4.
- All communication layers and components which use an identification information as shown in Figure 5 shall register for the ID Change Notifications using the Subscribe ID change Notification service. When the Security Entity indicates an identifier change event, all registered layers shall invoke a two-phase commit process. When the commit is successful, the communication layer shall change their identification.
- In the communication profile for CAM and DENM, all the layers' identifiers (MAC address, GN Source address, stationID) shall be derived from the identifier provided by the Security Entity in the ID Change Notification. If a shorter identifier is used by a layer, the least significant bits of the provided identifier (authorization certificate hash of type HashedID8) shall be used as the layer identifier.

NOTE: When the ITS-S changes ID for privacy reasons, the GN address is updated as specified in ETSI EN 302 636-4-1 [10]. Only the last field of the address (MAC ID of length 48 bits) is updated and derived from the pseudonym.

[Itss_WithPrivacy] the ITS-S shall use Lock ID Change service to ask the security entity to block the pseudonym / ID change for the duration specified in number of seconds. The lock will be released automatically afterwards or can be released by using the Unlock ID Change service. The Lock and Unlock Change service should be provided at SF or SN SAP.

The detailed requirements of this Identity Management procedure (use and change of ITS station's pseudonym) are specified in ETSI TS 102 941 [5] and the SAP primitives supporting Identity Management can be found in ETSI TS 102 723-8 [i.7].

6.6 Confidentiality

Many of the applications and services described in ETSI TR 102 638 [i.1] and summarized in table 2 are based on the transmission of broadcast messages which are intended to be viewed and processed by all recipients. Consequently, there are no confidentiality requirements associated with these messages other than the protection of the sender's identity. However, there are some applications and services which will use point-to-point unicast communications and which will contain sensitive information of a personal or commercial nature. These services will require access to security services that can ensure that this information can only be viewed by the intended recipient(s).

The confidentiality of transmitted information is protected primarily by the encryption of messages within an established security association such that it can only be decrypted by the recipient to whom it is addressed.

The true identity of the sender of broadcast ITS messages is kept confidential by ensuring that all such messages are sent pseudonymously.

The detailed requirements of these confidentiality procedures are specified in ETSI TS 102 943 [7] and the protocols required to support them can be found in ETSI TS 102 941 [5].

7 ITS Security management system

7.0 General

This clause presents the global architecture of the Cooperative-ITS Security Certificate Management System (also named C-ITS Trust Model), its functional entities and the list of services and interfaces that shall be provided by the C-ITS Trust Model to support the life-cycle management of Trusted C-ITS Stations.

The Cooperative-ITS Security Certificate Management System architecture is depicted in Figure 11.

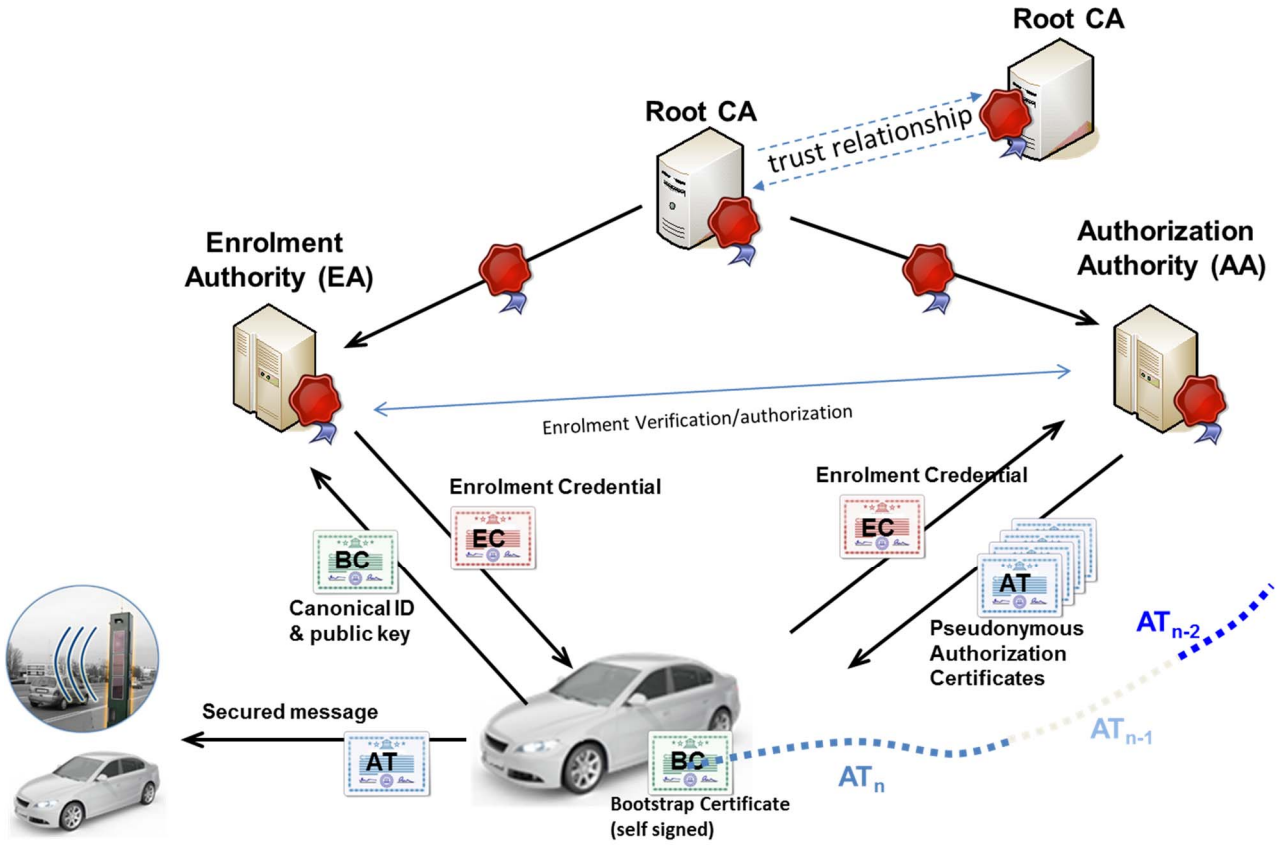


Figure 11: PKI architecture

NOTE 1: The Security Management System entities and functions which are related to the ITS-S Misbehaviour Detection (MBD), the revocation of ITS-S enrolment credentials in the EA where the ITS-S has been enrolled beforehand, and the process to support migration and agility of the cryptographic system as well as security updates of the ITS-S platform is out of scope of the present document.

Each of the functional elements in the PKI 'single root CA' trust model has a specific role to play and these are summarized in Table 8.

The C-ITS Security Management System may allow operation of one or multiple Root CAs. Different trust model options can be considered for the ITS Security Management System architecture and are presented and evaluated in the context of the European C-ITS Platform WG5 report [i.8], Annex 1. This may include possible options such as:

- Single Root CA
- Cross-certification
- Bridge CA
- Certificate Trust List

Table 8: Functional element roles of the PKI

Functional element	Description
Root Certification Authority	The Root CA is the highest level CA in the certification hierarchy. It provides EA and AA with proof that it may issue enrolment credentials, respectively authorization tickets
Enrolment Authority	Security management entity responsible for the life cycle management of enrolment credentials. Authenticates an ITS-S and grants it access to ITS communications
Authorization Authority	Security management entity responsible for issuing, monitoring the use of authorization tickets. Provides an ITS-S with authoritative proof that it may use specific ITS services
Distribution Center (optional)	Provides to ITS-S the updated trust information necessary for performing the validation process to control that received information is coming from a legitimate and authorized ITS-S or a PKI certification authority by publishing the CTL and CRL
Sending ITS-S	Acquires rights to access ITS communications from Enrolment Authority Negotiates rights to invoke ITS services from Authorization Authority Sends single-hop and relayed broadcast messages
Relaying ITS-S	Receives broadcast message from the sending ITS-S and forwards them to the receiving ITS-S if required
Receiving ITS-S	Receives broadcast messages from the sending or relaying ITS-S
Manufacturer	Installs necessary information for security management in ITS-S at production
Operator	Installs and updates necessary information for security management in ITS-S during operation

NOTE 2: The Root CA stores its security certificates information and the trusts list information (CRL, CTL) in a local repository. Optionally the Distribution Center may be used to distribute these information to all the PKI participants.

7.1 Certificate Trust List/multiple Root CAs

In the present document, when multiple Root CAs exist and cooperate within the C-ITS Trust Domain, the C-ITS Security Management System shall follow the Certificate Trust List approach.

In Europe, the top-level governance roles are defined in C-ITS Platform Certificate Policy document. The entities responsible for the trust management of the C-ITS system (i.e. governing all aspects related to the operational PKI) are:

- Policy Authority
- Trust List Manager
- C-ITS Point Of Contact (CPOC)

as described in Table 9.

Table 9: Functional element roles of the top-level trust management

Functional element	Description
Policy Authority	Policy authority is a role composed by the representatives of public and private stakeholders (e.g. Authorities, Road Operators, Vehicle Manufacturers, etc.) participating to the C-ITS trust model. It designates and authorizes the TLM and the CPOC to operate in the C-ITS Trust system. It decides if root CAs are trustable and approves/removes the Root CAs operation in C-ITS trust domain by notifying the TLM about approved/revoked Root CAs certificates
Central Point Of Contact (optional)	The CPOC is a unique entity appointed by the Policy Authority. It has responsibility to establish and contribute to ensure communication exchange between the Root CAs, to collect the Root CA certificates and provide them to the Trust List Manager (TLM). The CPOC is also responsible for distributing the ECTL to any interested entities in the trust model
Trust List Manager	Trust List Manager is responsible for creating the list of root CA certificates and TLM certificates and signing it. The signed list issued by the TLM is called the ECTL

NOTE 1: The Policy Authority is the top level role of the C-ITS Trust system. It is responsible for certificate policy management and for the management of the C-ITS Trust system operational entities such as the TLM, the CPOC and the Root CAs.

NOTE 2: The TLM stores its security certificates information and the trusts list information (ECTL) in a local repository. Optionally the CPOC may be used to distribute these information to all the PKI participants.

Information is exchanged between the functional elements in the ITS security reference model across the reference points identified in table 10. The characteristics of each of these are summarized in Table 11 and the UML components model is given in Figure 12.

Table 10: Summary of ITS security reference points

Reference point	Security services supported
S_1	Establish Security Association
	Update Security Association
	Send secured message
	Receive secured message
	Remove Security Association
	Confidentiality services
	Integrity services
	Replay protection services
S_2	Obtain authorization tickets
	Update authorization tickets
	Publish authorization status
	Update local authorization status repository
	Report misbehaving ITS-S
S_3	Obtain enrolment credentials
	Update enrolment credentials
	Remove enrolment credentials
	Remote activate ITS transmission
	Remote deactivate ITS transmission
	Report misbehaving ITS-S
S_4	Obtain authorization tickets
	Update authorization tickets
	Publish authorization status
	Update local authorization status repository
S_5	Provide credential of security management entities
	Provide status of authorization of security management entities (CTL, CRL CAs)
S_6	Provide security management entity credentials
	Provide status of authorization of security management entities (CTL, CRL CAs)
S_7	Provide security management entity credentials
S_8	Provide security management entity credentials
S_9	Issue security management entity credentials
	Provide status of authorization of security management entities (CTL, CRL CAs)
S_{10}	Issue security management entity credentials
	Provide status of authorization of security management entities (CTL, CRL CAs)
S_{11}	Provide/issue Root CA credentials
S_{12}	Provide ECTL to all participants of the trust domain (RCAs, EAs, AAs; DCs, ITS-Ss)
Internal - confidentiality (see note)	Authorize single message
	Validate authorization on single message
	Encrypt single message
	Decrypt single message
Internal - Integrity (see note)	Calculate check value
	Insert check value
	Validate check value
	Validate data plausibility

Reference point	Security services supported
Internal - replay protection (see note)	Time-stamp message
	Sequence number message
Internal - accountability (see note)	Record incoming message in audit log
	Record outgoing message in audit log
Internal - Identity Management (see note)	Lock ID Change
	Unlock ID Change
	Subscribe ID change Notification
	Unsubscribe ID change Notification
	ID Change Notification
	Trigger ID Change
NOTE: These services are required to support ITS communications security services but do not involve the exchange of information across one of the reference points.	

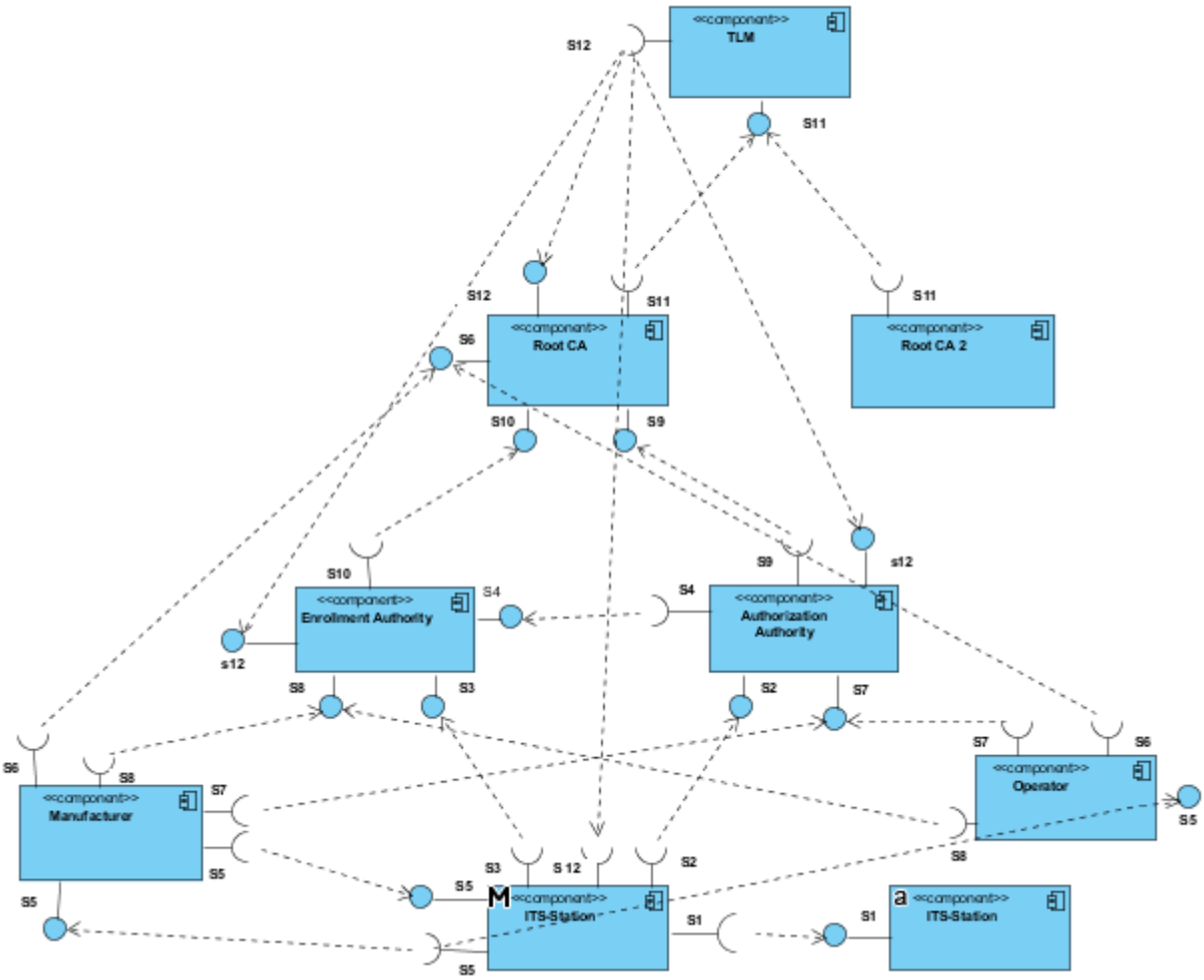


Figure 12: Reference points between functional elements

NOTE 3: The CTL information on reference point S12 is published by the TLM and made available in read access to all participants of the C-ITS Trust Domain. For sake of clarity, the interfaces S12 with Manufacturers, EAs, AAs and ITS Stations are not depicted in the UML diagram.

The information passing across each ITS security reference point supports a range of the communications security services specified in Table 11.

Table 11: Communications security services supported at ITS security reference points

Reference Point	Functional Element		Information carried
	From	To	
S_1	Sending ITS-S	Receiving ITS-S	Message payload such as: CAM defined in ETSI EN 302 637-2 [2], SPATEM defined in ETSI TS 103 301 [9], MAPEM defined in ETSI TS 103 301 [9], IVIM defined in ETSI TS 103 301 [9], SREM defined in ETSI TS 103 301 [9], SSEM defined in ETSI TS 103 301 [9].
	Sending ITS-S	Relaying ITS-S	Message payload such as: DENM defined in ETSI EN 302 637-3 [3], SPATEM defined in ETSI TS 103 301 [9], MAPEM defined in ETSI TS 103 301 [9], IVIM defined in ETSI TS 103 301 [9], SREM defined in ETSI TS 103 301 [9], SSEM defined in ETSI TS 103 301 [9].
	Relaying ITS-S	Receiving ITS-S	Message payload such as: DENM defined in ETSI EN 302 637-3 [3], SPATEM defined in ETSI TS 103 301 [9], MAPEM defined in ETSI TS 103 301 [9], IVIM defined in ETSI TS 103 301 [9], SREM defined in ETSI TS 103 301 [9], SSEM defined in ETSI TS 103 301 [9].
S_2	ITS-S	Authorization Authority	Requests for authorization to invoke ITS security services, see ETSI TS 102 731 [4].
	Authorization Authority	ITS-S	Contact information of AA AA Credentials Authorization tickets, see ETSI TS 102 731 [4].
S_3	ITS-S	Enrolment Authority	Request for permission to access ITS communications, see ETSI TS 102 731 [4] and clause 6.4.
	Enrolment Authority	ITS-S	Contact information of EA EA Credentials Enrolment credentials, see ETSI TS 102 731 [4].
S_4	Authorization Authority	Enrolment Authority	Request for verification of ITS-S enrolment credentials, see ETSI TS 102 731 [4].
	Enrolment Authority	Authorization Authority	Verification of ITS-S enrolment credentials, see ETSI TS 102 731 [4].
S_5	ITS-S	Manufacturer	Canonical Identity and associated public key, see ETSI TS 102 941 [5] (see note 1).
	Manufacturer	ITS-S	Canonical Identity and associated public key, see ETSI TS 102 941 [5] (see note 1).
	Manufacturer/Operator	ITS-S	Contact information of EAs and AAs. Credentials of Root CAs. Credentials of EAs and AAs.
S_6	Root CA	Manufacturer/Operator	Credentials of Root CA, see ETSI TS 103 097 [8]. Contact information of EAs and AAs. Credentials of EAs and AAs, see ETSI TS 103 097 [8]. Revocation status of EAs and AAs (for example CRL which indicates the authorization status of subordinate CAs controlled by the Root CA).
S_7	Authorization Authority	Manufacturer/Operator	Contact information of AA. AA Credentials, see ETSI TS 103 097 [8].
S_8	Manufacturer	Enrolment Authority	Canonical Identity and associated public key, see ETSI TS 102 941 [5].
	Enrolment Authority	Manufacturer/Operator	Contact information of EA. EA Credentials ETSI TS 103 097 [8].
S_9	Authorization Authority	Root CA	Request for AA Credentials (see note 2)
	Root CA	Authorization Authority	AA Credentials, see ETSI TS 103 097 [8] (see note 2). Update of trust information list (EA and AA certificates). Revocation status of EAs and AAs (CRL CAs).

Reference Point	Functional Element		Information carried
	From	To	
S_{10}	Enrolment Authority	Root CA	Request for EA Credentials (see note 2).
	Root CA	Enrolment Authority	EA Credentials, see ETSI TS 103 097 [8] (see note 2). Update of trust information list (EA and AA certificates). Revocation status of EAs and AAs (CRL CAs).
S_{11}	Root CA	TLM	Provide Root CA Credential for approval and insertion in ECTL.
S_{12}	TLM	all	Publish list of approved and revoked Root CA certificates (ECTL).

NOTE 1: In the initialization process, the ITS-S station is provisioned with a unique identifier (canonical identity) and associated credentials used for identification management of the ITS-S by the PKI. These credentials consist at least of a public and private cryptographic key pair. In the reference point description, there are two ways for providing these credentials:
- either the ITS-S canonical key pair is generated internally in the ITS-S security module (HSM) and communicated to the Manufacturer in a secure way; or
- the Manufacturer generates the canonical key pair in the manufacturing system, provision it to ITS-S using a secure channel and then delete this key in the manufacturing system to avoid any risk of leakage and stealing of ITS-S identity credentials.

NOTE 2: These services supported by the Root CA are provided as off-line operations.

7.2 Root CA

Each CA hierarchy (for EA or AA) has at its summit a Root CA, which is the ultimate root of trust for all certificates within that hierarchy.

The RCA shall be able to update the list of trusted sub CA certificates and to revoke a sub CA certificate within its hierarchy.

A RCA shall always be used off-line and never be connected to any network.

NOTE 1: In the present document, CRLs issued by a RCA are certificate revocation list for authorities (CRL CA).

The functions provided by the RCA shall be as follows:

- Issuing CAs certificates for EA or AA;
- Creation, renewal and distribution of the Root CA certificates;
- Revocation of CA certificates (EA or AA) at the end of life or in case of an exception (e.g. compromising of the CA private keys);
- Generation and issuance of the signed lists (CRL and CTL);
- Generation of log files of the RCA operational activities for auditing purpose.

When a RCA is used as a Trust anchor for the ITS-S, the RCA certificate shall be transmitted to the ITS-S for initialization using a secure communication channel, e.g. during the manufacturing process.

NOTE 2: For ITS communications, it is assumed that each trusted ITS-S is fulfilling the ITS-S communication security requirements specified in clause 6.

In order to trust an incoming message, an ITS-S shall have secure access at least to the root certificate at the summit of the hierarchy for the authorization ticket attached to the message. The ITS-S may obtain root certificates during the manufacture or maintenance lifecycle stages. In principle root certificate information may be distributed over the air through a cross-certification process, a bridge CA or a trusted certificates list (CTL).

NOTE 3: The present document only considers the Certificate Trust List approach.

The Root CA shall store the Root CA certificates and the trust list information (CRL, CTL) in a local repository. It may also store the DC access information (URL) in its local repository, if DC is present.

The local repository shall give a READ access to all local users and applications without restriction. The local repository shall allow WRITE access to only authorized, authenticated users. The local repository may be accessed via a dedicated communication channel in a way securing the authenticity and integrity of the data.

The Distribution Center (DC) may optionally be provided. If present, the following requirements apply:

- The DC shall ensure the access to trust list information (CTLs, CRLs) to all entities of the PKI hierarchy managed by the Root CA.
- The DC shall provide an unrestricted read access to the trust lists.
- The DC shall provide a write access to the lists only for authorized, authenticated users.
- If multiple Root CAs are operating within the C-ITS Trust model, the DC may give access to ECTL.
- If multiple Root CAs are operating within the C-ITS Trust model, the DC may give access to CRLs of other Root CAs.

7.3 Enrolment Authority

The EA issues a proof of identity after authenticating the requesting ITS-S, in the form of an Enrolment Credential. The proof of identity does not reveal the canonical identifier to a 3rd party and shall be used by the ITS-S to request authorization of services from an AA.

NOTE 1: The manufacturer or device operator is in charge of the generation of the ITS-S canonical identity/credentials in a secured environment. See clause 6.4 and Table 11 for detailed requirements.

The functions provided by the EA shall be as follows:

- Registration of ITS-S, management of ITS status and permissions, management of their cryptographic certificates (EC) indicating the applications, services and capabilities that the ITS-S is granted to use.
- Issuing Enrolment Certificates to ITS-S after authenticating the requesting ITS-S.
- Revocation of the ITS-S enrolment credentials at the end of life or in case of an exception (e.g. compromising of the ITS-S private keys, etc.).
- Creation, renewal of EA certificates: the EA may generate the key pairs, generate the certificate request, and transfer the application form to the RCA.
- Verification that the ITS-S has necessary permissions and is trusted when requesting authorization tickets.
- Update the trust information lists issued by RCAs through the DC or the local repository and, update the ECTL, if TLM is set up.
- Generation of log files of the EA operational activities for auditing purpose.

NOTE 2: The requirements and procedures for CA application to a Root CA are specified in detail in ETSI TS 102 941 [5].

7.4 Authorization Authority

An ITS-S that has been enrolled with, and been authenticated by an EA shall apply to an AA for specific permissions within the enrolment authority's domain and the AA's authorization context. These privileges are denoted by means of authorization tickets. Each authorization ticket specifies a particular authorization context which comprises a set of permissions.

EXAMPLE: An authorization ticket might grant permission to an ITS-S to broadcast messages from a particular message set. Alternatively, it might grant permission to claim certain privileges.

NOTE 1: An AA will normally be responsible for a particular set of contexts which may be specified by one or more of the following:

- application (for example, cooperative awareness applications for personal user vehicles, emergency service vehicles or tolling);
- application permissions which allows to grant permission to certain privileges or not;
- time period;
- geographic region (nation, state, locality); or
- any other criteria that can be encoded.

To protect privacy of the ITS-S, an AA shall have no knowledge of the long-term identity (EC) of the ITS-S, and the Enrolment Authority shall not be able to link the short term identity (AT) to the long term identity (EC) of the ITS-S.

The functions provided by the AA shall be as follows:

- Issuing Authorization Tickets to the ITS-S after authenticating and authorizing the AT request by the EA;
- Creation, renewal of AA certificates: the AA may generate the key pairs, generate the certificate request, and transfer the application form to the RCA;
- Verification that the ITS-S has necessary permissions and is trusted when requesting authorization tickets;
- Update the trust information lists issued by RCAs through the DC or the local repository and, update the ECTL, if TLM is set up;
- Generation of log files of the EA operational activities for auditing purpose.

NOTE 2: The requirements and procedures for CA application to a Root CA are specified in detail in ETSI TS 102 941 [5].

7.5 Trust List Manager

The functions provided by the TLM shall be as follows:

- Creation and renewal of the TLM certificates.
- Distribution of TLM certificates via a local repository or via the CPOC.
- Insertion or removal of Root CA certificates in the ECTL (after approval by the Policy Authority, e.g. when a RCA certificate is created, renewed or revoked).
- Creation of the signed list of root CA certificates and TLM certificates (ECTL).
- Distribution of ECTL to all participants of the C-ITS trust domain via a local repository or via the CPOC.
- Generation of log files of the TLM operational activities for auditing purpose.

NOTE: The CPOC is mandatory in the EU Certificate Policy [i.9].

Annex A (informative): Change history

Date	Version	Information about changes
June 2012	1.1.1	First version of the TS
November 2016	1.2.1	Revised ITS station security services enabling simultaneous change of pseudonym and communication IDs for privacy
April 2018	1.3.1	Security architecture revised; allow multiple interoperable RCAs using a Certificate Trust List concept

History

Document history		
V1.1.1	June 2012	Publication
V1.2.1	November 2016	Publication
V1.3.1	April 2018	Publication