ETSI TS 102 940 V1.1.1 (2012-06)

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

Reference
DTS/ITS-0050014

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

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

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

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Intelligent Transport System (ITS).

1 Scope

The present document specifies a security architecture for Intelligent Transport System (ITS) communications. Based upon the security services defined in 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 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

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 http://docbox.etsi.org/Reference.

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

2.1 Normative references

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

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

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

[3] ETSI TS 102 637-3: "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".

2.2 Informative references

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

[i.1] 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 FprCEN/TS 16439: "Electronic fee collection - Security framework".

[i.5] ETSI TS 102 890-2: "Intelligent Transport Systems (ITS); Facilities layer function; Services announcement specification".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

authorization authority: authority that provides an ITS-S with permission to invoke ITS applications and services

canonical identifier: structured identifier that is globally unique

enrolment authority: authority that validates that an ITS-S can be trusted to function correctly

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

BSA	Basic Set of Applications
CA	Co-operative Awareness
CAM	Co-operative Awareness Message
CN	Co-operative Navigation
CS	Communities Services
CSM	Co-operative Speed Management
DENM	Decentralized Environment Notification Message
EA	Enrolment Authority
IP	Internet Protocol
IPv6	Internet Protocol version 6
ITS	Intelligent Transport System
ITS-S	ITS Station
LBS	Location Based Services
LCM	Life Cycle Management
OSI	Open System Interconnect
PDA	Personal Data Appliance
PKI	Public Key Infrastructure
RHW	Road Hazard Warning
RSU	Road Side Unit
TTP	Trusted Third Party
WAVE	Wireless Access in Vehicular Environments
WSA	WAVE Service Announcement

4 ITS reference architecture

EN 302 665 [1] describes an ITS station architecture based upon 4 processing layers identified as follows:

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

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

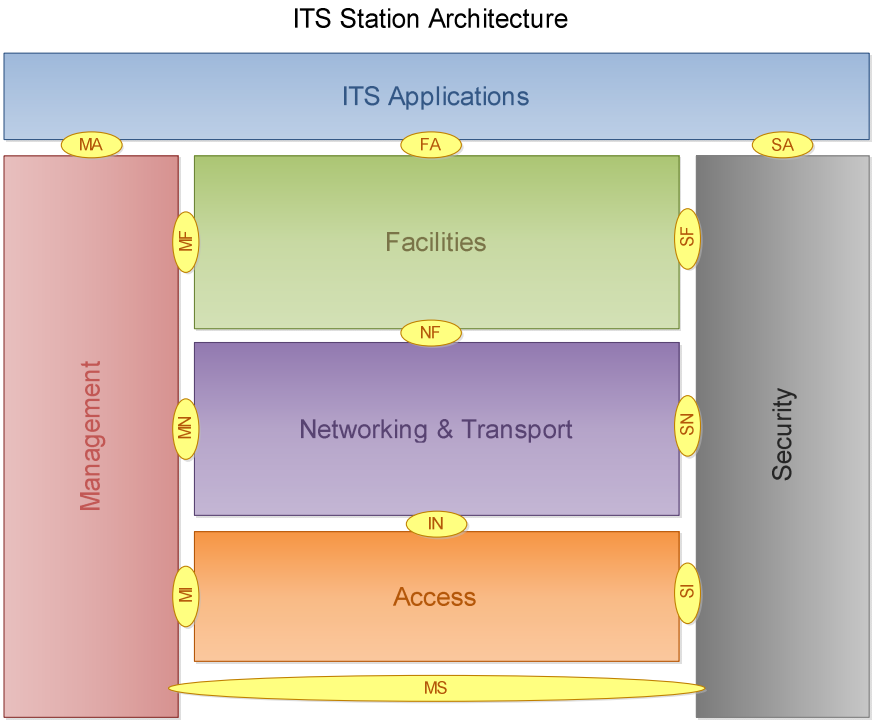


Figure 1: ITS station architecture (from EN 302 665 [1])

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

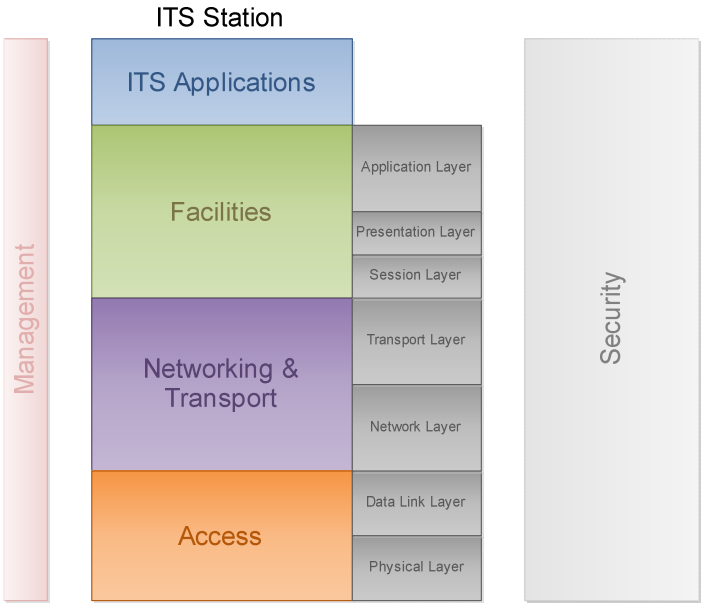


Figure 2: Mapping of OSI modelling layers to the ITS architectural layers

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

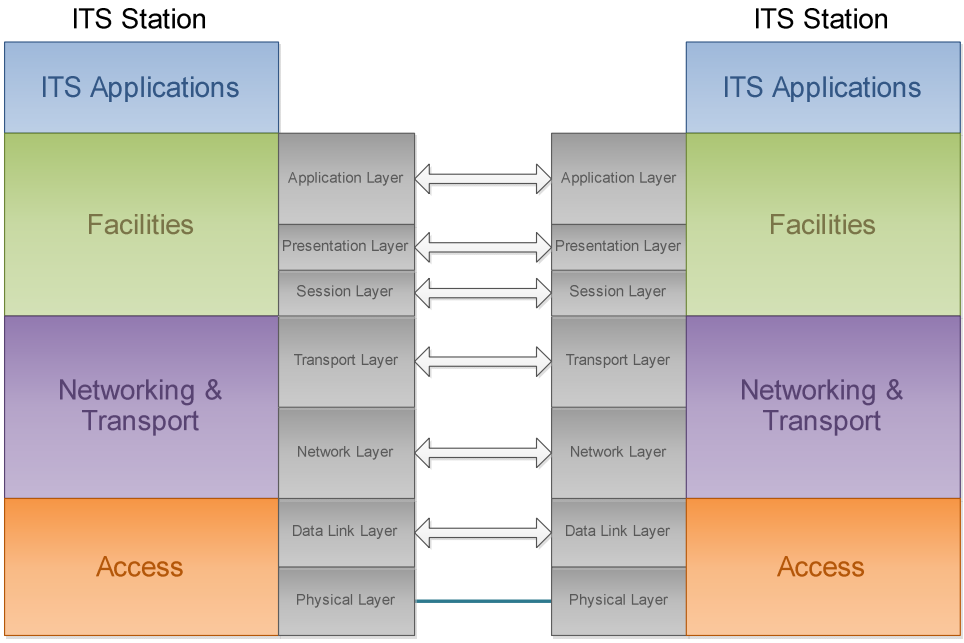


Figure 3: ITS communications architecture

4.1 ITS applications groups

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 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 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]	

4.1.1 Summary of ITS applications

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

Table 2: ITS applications communication behaviour

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

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;

4.1.1.1 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

4.1.1.2 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.

4.1.1.3 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

4.1.1.4 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.

4.1.1.5 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] (IEEE Vehicular Technology Society 2010a) but does not preclude any alternative method of providing Service Announcements including ETSI Facilities service announcement 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.

4.1.1.6 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).

4.1.1.7 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.

EXAMPLE: 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.

4.1.1.8 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.

4.1.1.9 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.

EXAMPLES: 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.

4.1.1.10 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).

4.1.2 Security requirements of ITS application groups

4.1.2.1 Security requirements of cooperative awareness

4.1.2.1.1 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.

4.1.2.1.2 Confidentiality

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

4.1.2.1.3 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 mechanisms and policies provided to protect privacy are given in TS 102 941 [5].

4.1.2.2 Security requirements of static local hazard warnings

4.1.2.2.1 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.

4.1.2.2.2 Confidentiality and Privacy

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

4.1.2.3 Security requirements of dynamic local hazard warnings

4.1.2.3.1 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.

4.1.2.3.2 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.

4.1.2.4 Security requirements of area hazard warnings

4.1.2.4.1 Authentication and Authorization

Authorization for area hazard warnings (Decentralized Environment Notification Messages, 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.

4.1.2.4.2 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.

4.1.2.5 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.

4.1.2.6 Security requirements of multiple applications

4.1.2.6.1 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 with in policies associated with the authorization or during the authorization process itself.

4.1.2.6.2 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 Security architecture

5.1 ITS station security architecture

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 4.

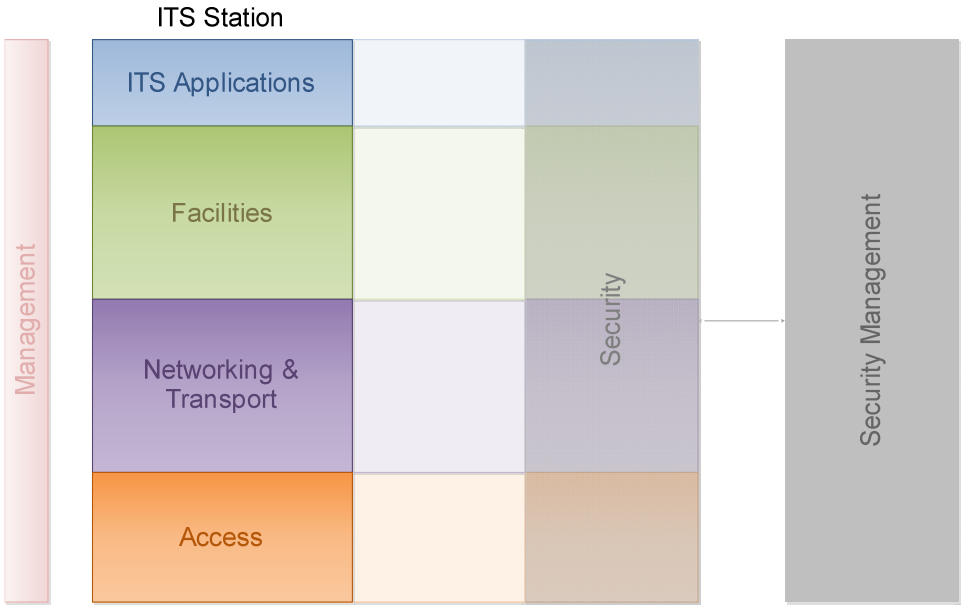


Figure 4: Architectural ITS security layers

5.2 Security services

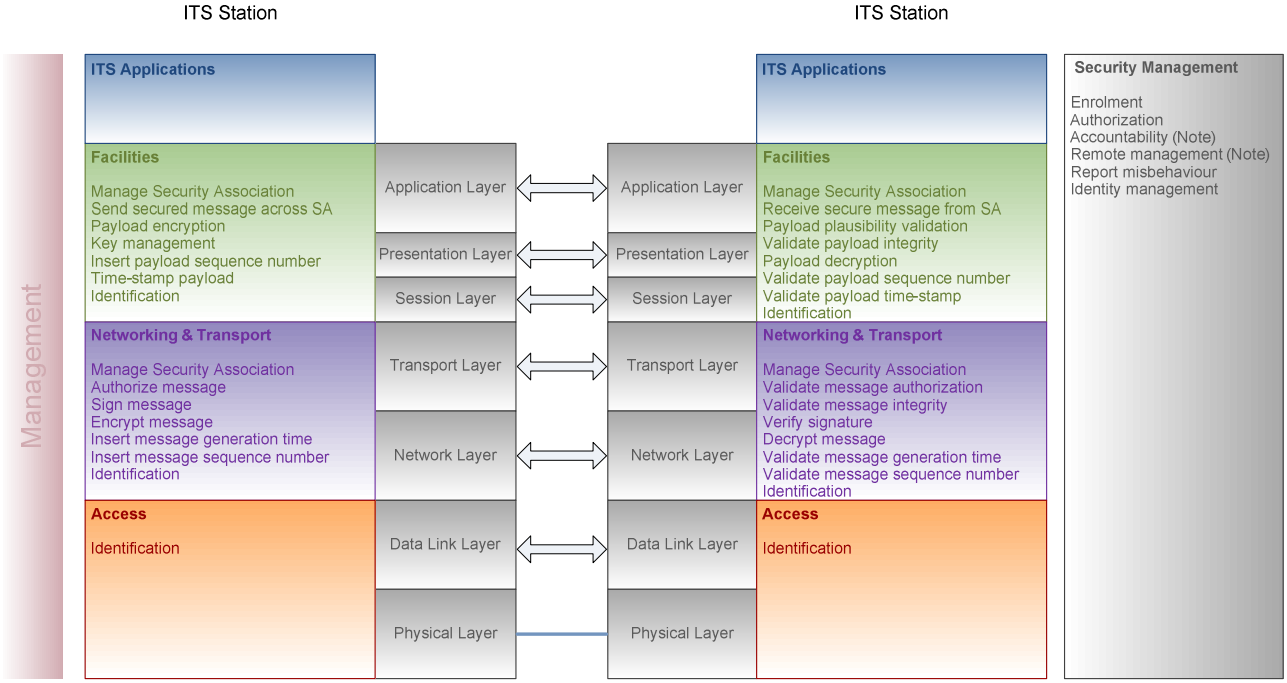
TS 102 731 [4] identifies a range of security services which may be supported by an ITS station in order to provide communications security between itself and other stations. Table 3 summarizes these services.

Table 3: ITS Security Services

Service category	Security service
Enrolment	Obtain Enrolment Credentials
	Update Enrolment Credentials
	Remove Enrolment Credentials
Authorization	Obtain Authorization Tickets
	Update Authorization Tickets
	Publish Authorization Status
	Update Local Authorization Status Repository
Security Associations management	Establish Security Association
	Update security association
	Send Secured Message
	Receive Secured Message
	Remove security association
Single message services	Authorize Single Message
	Validate Authorization on Single Message
	Encrypt Single Message
	Decrypt Single Message
Integrity services	Calculate Check Value
	Validate Check Value
	Insert Check Value
Replay Protection services	Replay Protection Based on Timestamp
	Replay Protection Based on Sequence Number
Accountability services	Record Incoming Message in Audit Log
	Record outgoing message in Audit Log
Plausibility validation	Validate Data Plausibility
Remote management	Remote Activate Transmission
	Deactivate ITS transmission
Report Misbehaving ITS-S	Report misbehaviour

5.3 ITS communications security architecture

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



NOTE: 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

5.4 ITS security reference 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 PDAs.

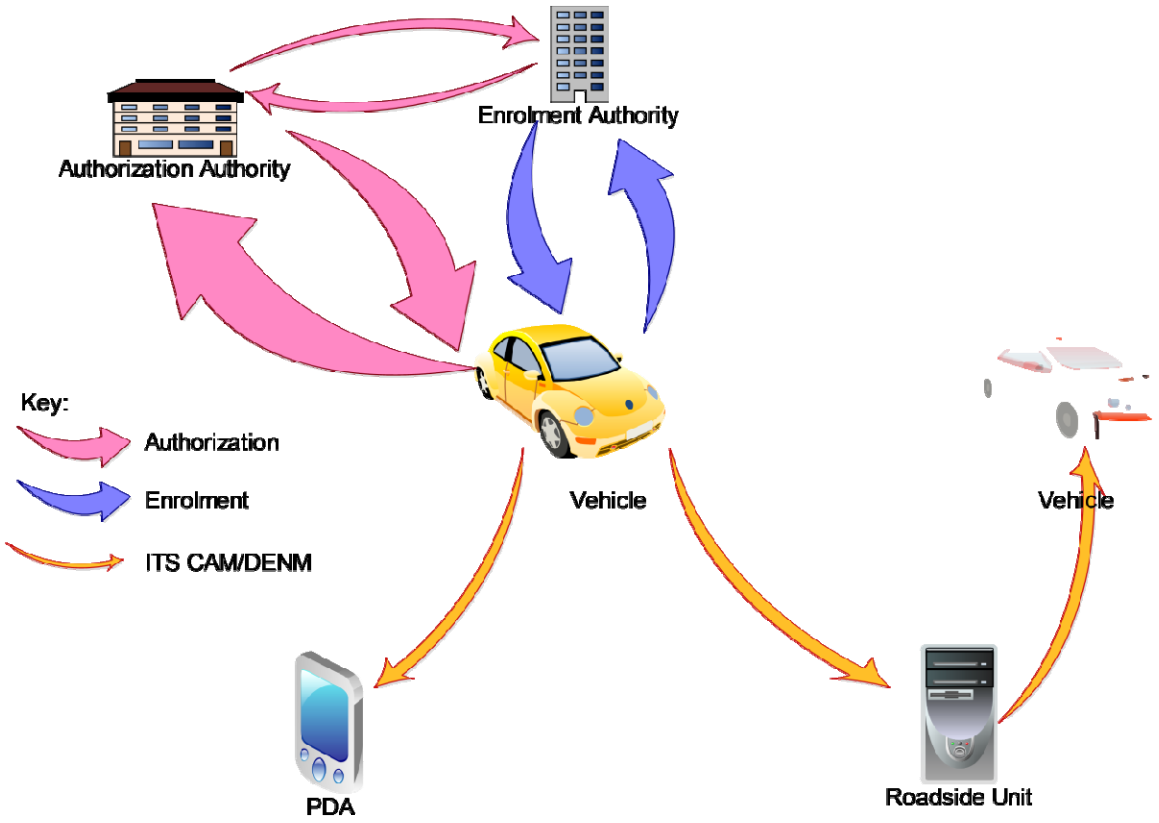


Figure 6: ITS communications reference scenario

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.

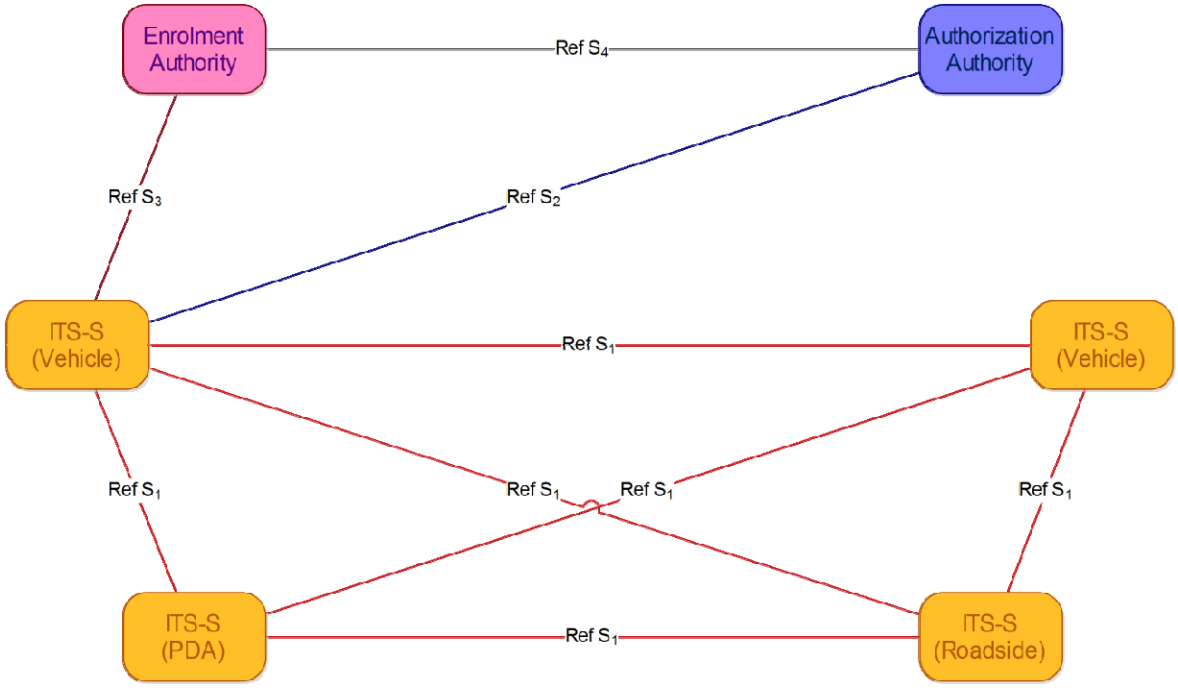


Figure 7: ITS security functional elements and reference points

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 at such a time 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).

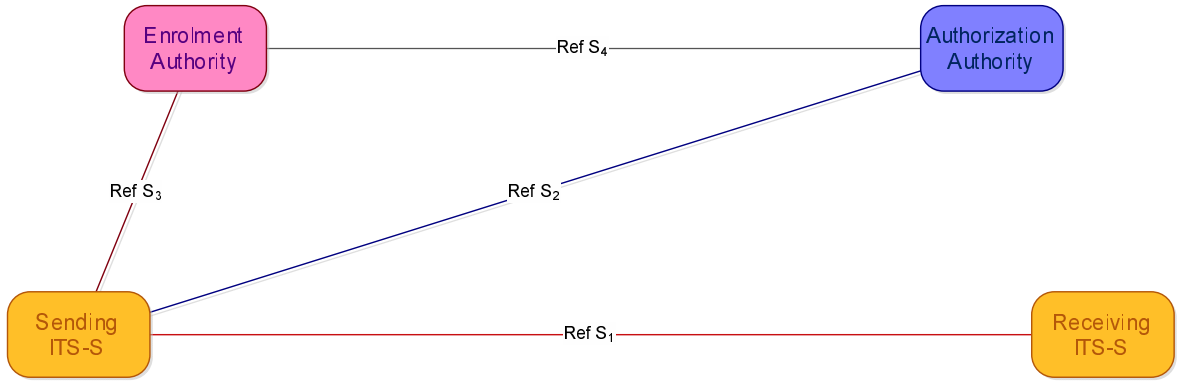


Figure 8: ITS security reference model for CAM

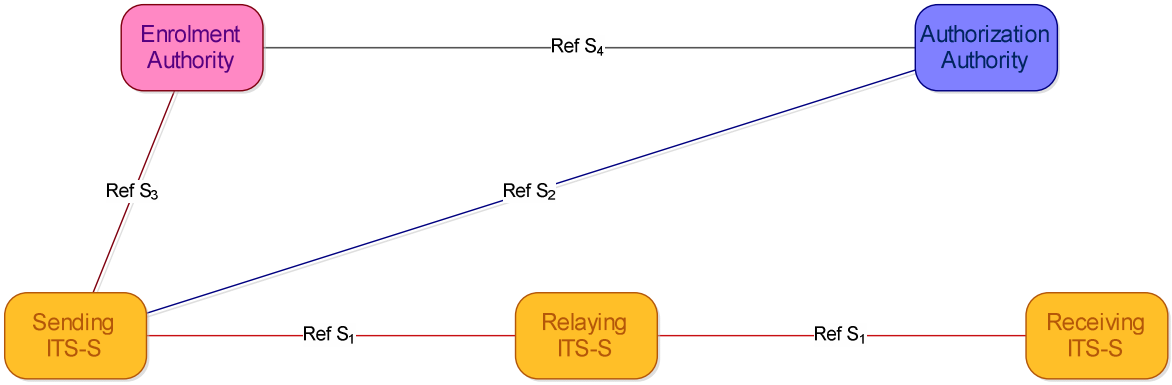


Figure 9: ITS security reference model for DENM

5.4.1 Security functional elements

Each of the functional elements in the ITS security reference models has a specific role to play and these are summarized in Table 4.

Table 4: 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

5.4.2 Security reference points

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 this are summarized in Table 5.

Table 5: Summary of ITS security reference points

Reference Point	Functional Element		Information carried
	From	To	
S_1	Sending ITS-S	Receiving ITS-S	CAM [2]
	Sending ITS-S	Relaying ITS-S	DENM [3]
	Relaying ITS-S	Receiving ITS-S	DENM [3]
S_2	Sending ITS-S	Authorization Authority	Requests for authorization to invoke ITS security services [4]
	Authorization Authority	Sending ITS-S	Authorization parameters [4]
S_3	Sending ITS-S	Enrolment Authority	Request for permission to access ITS communications [4]
	Enrolment Authority	Sending ITS-S	Enrolment credentials [4]
S_4	Authorization Authority	Enrolment Authority	Request for verification of ITS-S enrolment credentials [4]
	Enrolment Authority	Authorization Authority	Verification of ITS-S enrolment credentials [4]

The information passing across each ITS security reference point supports a range of the communications security services specified in Table 3. The distribution of security services to the reference points is specified in Table 6.

Table 6: 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 (note 1)
	Remote deactivate ITS transmission (note 1)
	Report misbehaving ITS-S
S_4	Obtain authorization tickets
	Update authorization tickets
	Publish authorization status
	Update local authorization status repository
Internal - confidentiality (note 2)	Authorize single message
	Validate authorization on single message
	Encrypt single message
	Decrypt single message
Internal - Integrity (note 2)	Calculate check value
	Insert check value
	Validate check value
	Validate data plausibility
Internal - replay protection (note 2)	Time-stamp message
	Sequence number message
Internal - accountability (note 2)	Record incoming message in audit log (note 1)
	Record outgoing message in audit log (note 1)
NOTE 1: The legality of these services is unclear and requires further study before the services can be fully specified. NOTE 2: 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 6.1.1). The basic requirements and procedures for enrolment are more specified in detail in TS 102 941 [5].

6.1.1 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 within the constraints of an appropriate authorization mechanism. Figure 10 shows, in generic terms, how this could be structured.

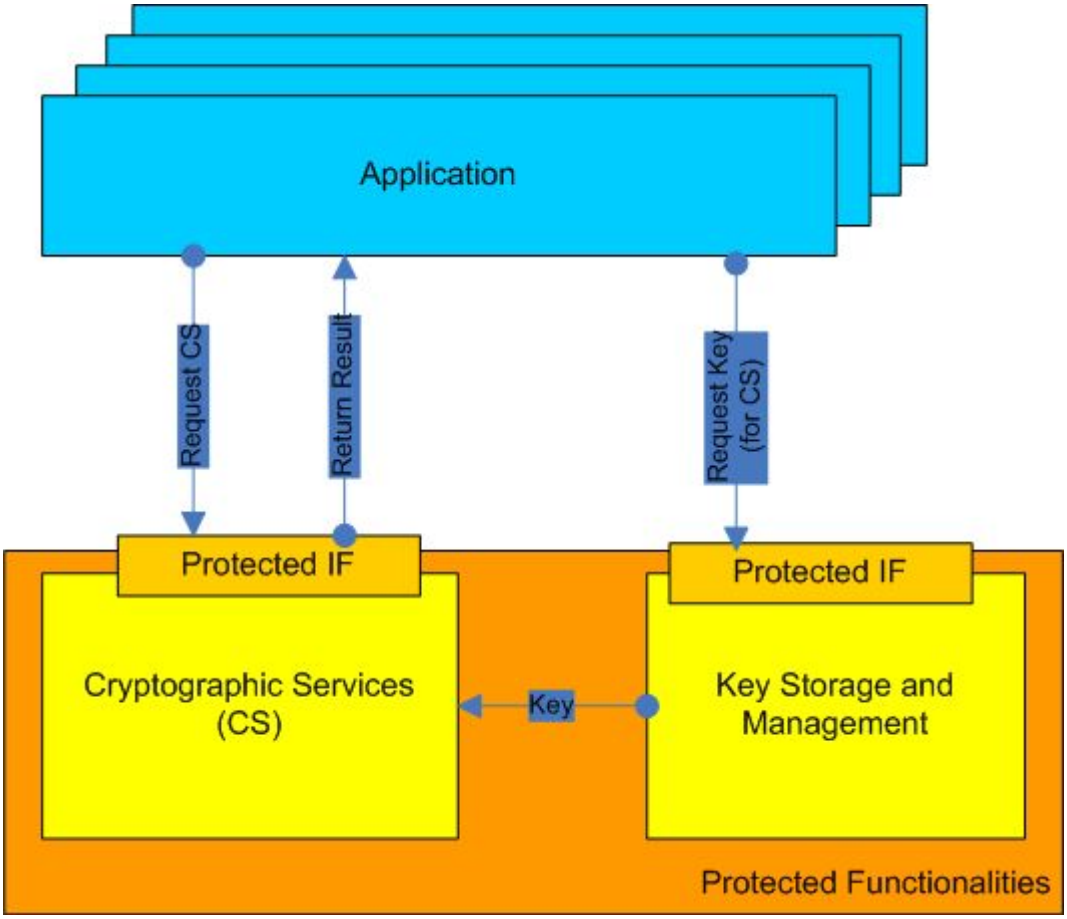


Figure 10: Schematic view of basic service protection for ITS-S station security

- 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.

6.2 Trust and privacy management

The enrolment and authorization services (Table 3) 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 TS 102 941 [5].

6.3 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 certificates 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 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);
    - a cryptographic 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 initialization credentials to establish a set of 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 certificate which, when combined 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 TS 102 942 [6] and the protocols required to support it can be found in TS 102 941 [5].

6.4 Confidentiality

Many of the applications and services described in the ITS BSA [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 they it 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 TS 102 943 [7] and the protocols required to support them can be found in TS 102 941 [5].

History

Document history		
V1.1.1	June 2012	Publication