ETSI TS 102 942 V1.1.1 (2012-06)

Intelligent Transport Systems (ITS);
Security;
Access Control

Reference
DTS/ITS-0050016

Keywords
ITS, security, service

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

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 authentication and authorization services to avoid unauthorized access to ITS services. It also specifies measures to ensure the required level of security and privacy for ITS message communication.

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

[2] ETSI TS 102 941: "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".

[3] ETSI TS 102 860: "Intelligent Transport Systems (ITS); Classification and management of ITS application objects".

[4] IEEE Std. 1609.2 draft D12 (January 2012): "Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages".

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.

Not applicable.

3 Definitions and abbreviations

3.1 Definitions

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

destination port: logical port number identifying the processing element to which a message received over the ETSI ITS Basic Transport Protocol should be directed within an ITS-S

ITS application object: generic term for either ITS application class, ITS application or ITS message set

3.2 Abbreviations

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

CAM	Cooperative Awareness Message
DENM	Decentralized Environmental Notification Message
ITS	Intelligent Transport System
ITS-S	ITS Station
PSID	Provider Service Identifier
RSU	Road Side Unit

4 Access Control in ITS

4.1 Authentication and Authorization requirements

TS 102 940 [1] identifies ITS application groups and their authorization requirements, as summarized below:

- Cooperative awareness:
  - 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.
- Static local hazard warning:
  - Authentication and Authorization requirements are similar to CAM with the addition that authorization should be limited to the specific purpose, functionality, and location of the respective RSU.
- Dynamic local hazard warning:
  - Authorization and Authentication requirements are similar to CAM with the addition that for the subsequent unicast session the local policies of the participating partners may require additional authorization and/or authentication. These additional requirements are out of scope of the present document.

- Area hazard warning:
  - 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.
- Advertised services, local high-speed unicast service, local multicast service, low-speed unicast service, distributed service:
  - Authentication and authorization services are service-specific.
- Considerations for multiple applications:
  - In general, Authentication and Authorization are handled separately for each individual application. The specific requirements need to be dealt with in policies associated with the authorization or during the authorization process itself.

4.2 Establishing preconditions within the ITS-S

Clause 5 in TS 102 941 [2] specifies the processes to be followed by an ITS-S in acquiring the necessary enrolment and authorization certificates. Clause 5.1 of TS 102 941 [2] defines the preconditions necessary within the ITS-S prior to enrolment. The same preconditions apply for authentication and authorization services.

5 Authentication and Authorization Services

5.1 Services for CAM

A message shall be identified as a CAM using the destination port number which shall be a two-byte port number preceded by the hexadecimal value 'DF' encoded in an ITS-AID [3] as shown in figure 1. The ITS-AID itself shall be encoded using the PSID defined in IEEE 1609.2 [4].

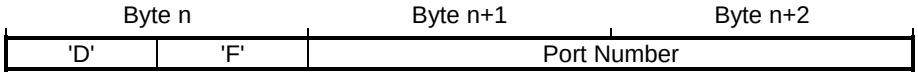

Figure 1: ITS port number carried in an ITS-AID

Authentication and authorization information (permissions) for CAMs are encoded in authorization certificates as defined in TS 102 941 [2]. CAMs shall include both of the following:

- the destination port number:
  - ensures that the message is routed to the appropriate processing element in the receiving ITS-S; and
- the associated authorization certificate or an unambiguous reference to it:
  - demonstrates to the receiving ITS-S that the sending ITS-S is authorized to invoke the sending of the received message type.

5.2 Services for DENM

A message shall be identified as a DENM using a port number encoded as shown in figure 1. The ITS-AID itself shall be encoded using the PSID defined in IEEE 1609.2 [4].

Authentication and authorization information (permissions) for DENMs are encoded in authorization certificates as defined in TS 102 941 [2]. DENMs shall include:

- the destination port number:
  - ensures that the message is routed to the appropriate processing element in the receiving ITS-S; and
- the associated authorization certificate or an unambiguous reference to it:
  - demonstrates to the receiving ITS-S that the sending ITS-S is authorized to invoke the sending of the received message type.

Annex A (informative): Bibliography

ETSI TS 102 943: "Intelligent Transport Systems (ITS); Security; Confidentiality services".

ISO 24102: "Intelligent transport systems - Communications access for land mobiles (CALM) - Management".

History

Document history		
V1.1.1	June 2012	Publication