ETSI TS 102 943 V1.1.1 (2012-06)

Intelligent Transport Systems (ITS);
Security;
Confidentiality services

Reference
DTS/ITS-0050017

Keywords
ITS, interoperability, 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

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 services to ensure that that the confidentiality of information sent to and from an Intelligent Transport System (ITS) station can be maintained at a level that is acceptable to the users of the station.

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 reference 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 133 102: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Security architecture (3GPP TS 33.102)".

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

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

[4] IEEE P1609.2/D12 (January 2012): "IEEE Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages".

NOTE: Available at: http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?reload=true&punumber=6140528.

[5] IETF RFC 2406, November 1998: "IP Encapsulating Security Payload (ESP)".

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 Abbreviations

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

2G	Second Generation mobile telephony
3G	Third Generation mobile telephony
ESP	Encapsulating Security Payload
G5A	Frequency band ranging from 5,875 GHz to 5,905 GHz
IP	Internet Protocol
ITS	Intelligent Transport System
ITS-S	ITS Station
LTE	Long Term Evolution

4 Confidentiality requirements

4.1 Confidentiality for different application groups

TS 102 940 [2] identifies ITS application groups and their confidentiality requirements, as summarized below:

- Cooperative awareness:

  No confidentiality services are needed.

- Static local hazard warning:

  No confidentiality services are needed.

- Dynamic local hazard warning:

  Depends on the details of the application. As no applications in this category have yet been fully specified, it is not possible to define confidentiality requirements.

- Area hazard warning:

  No confidentiality services are needed.

- Advertised services, local high-speed unicast service, local multicast service, low-speed unicast service, distributed service:

  Confidentiality services are service-specific.

- Considerations for multiple applications:

  The use of multiple applications does not impose additional requirements for confidentiality.

- Signalling data:

  An ITS-S should not reveal signalling data to unauthorised parties. Confidentiality services provide one mechanism that may be used to conceal the signalling data.

5 Confidentiality Services

5.1 Application Layer

The present document does not mandate specific confidentiality services for use at the application layer. Applications may use any appropriate confidentiality service, for example the data encryption services provided by IEEE P1609.2 [4].

5.2 Network Layer

5.2.1 IP

Confidentiality services for IPv6 shall be provided using the Encapsulating Security Payload (ESP) protocol within IPSec [5]. The key management services for IPv6 shall be as defined in TS 102 941 [3].

5.2.2 Basic Transport Protocol

No confidentiality services for the ITS Basic Transport Protocol are defined.

5.3 Link layer

5.3.1 5,9 GHz / 802.11p link

No mechanisms suitable for link-layer confidentiality over an ITS G5A link have been defined.

5.3.2 2G/3G/LTE

Confidentiality services for 2G/3G/LTE communications shall be provided by the mechanisms specified in TS 133 102 [1].

5.3.3 Other link layer protocols

Confidentiality mechanisms for communications over a link layer other than the link layers specified above shall provide at least 128 bits of cryptographic security.

Annex A (informative): Bibliography

IEEE 802.11p: "IEEE Standard for Information technology - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments".

History

Document history		
V1.1.1	June 2012	Publication