

ETSI TS 102 941 V1.1.1 (2012-06)



Intelligent Transport Systems (ITS); Security; Trust and Privacy Management

ETSI TS 102 941 V1.1.1 (2012-06)

<https://standards.iteh.ai/catalog/standards/etsi/2447776c-c889-48cf-b8a0-1c33ac318e98/etsi-ts-102-941-v1-1-1-2012-06>

Reference

DTS/ITS-0050015

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

(<https://standards.iteh.ai>)
Document Preview

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/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2012.
All rights reserved.

DECTTM, PLUGTESTSTM, UMTSTM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM and LTETM are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
GSM[®] and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	4
Foreword.....	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	6
3 Definitions and abbreviations.....	6
3.1 Definitions.....	6
3.2 Abbreviations	6
4 ITS authority hierarchy	7
4.1 Overview.....	7
4.2 ITS authorities	7
4.2.1 Enrolment Authority	7
4.2.2 Authorization Authority.....	8
4.2.3 Root CA	8
5 Privacy in ITS.....	8
6 Trust and privacy management	9
6.1 ITS-S Security Lifecycle	9
6.1.1 Manufacture.....	9
6.1.2 Enrolment	10
6.1.3 Authorization	10
6.1.4 Maintenance.....	10
6.2 Public Key Infrastructure	10
6.2.1 Assumption and requirements.....	10
6.2.2 Message Sequences.....	10
6.2.2.1 Introduction.....	10
6.2.2.2 Enrolment Request.....	11
6.2.2.3 Authorization Request.....	13
7 Security association and key management between ITS Stations.....	16
7.1 Broadcast SAs	16
7.2 Multicast SAs	16
7.3 Unicast SAs	17
Annex A (informative): ITS security messages specified in ASN.1.....	18
A.1 ITS trust and privacy messages specified in ASN.1.....	18
A.2 Enrolment and authorization message structures	18
Annex B (informative): Secret-key use cases and application categories.....	26
Annex C (informative): Extensions to IEEE 1609.2 to support additional security functions	27
C.1 Rationale.....	27
C.2 Use of a cryptographic digest of the signer identifier	27
C.3 Encryption of the signer identifier in an authorization certificate request	27
C.4 Request and transmission of multiple authorization certificates.....	28
Annex D (informative): Bibliography	29
History	30

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).

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TS 102 941 V1.1.1 \(2012-06\)](https://standards.iteh.ai/catalog/standards/etsi/2447776c-c889-48cf-b8a0-1c33ac318e98/etsi-ts-102-941-v1-1-1-2012-06)

<https://standards.iteh.ai/catalog/standards/etsi/2447776c-c889-48cf-b8a0-1c33ac318e98/etsi-ts-102-941-v1-1-1-2012-06>

1 Scope

The present document specifies the trust and privacy management for Intelligent Transport System (ITS) communications. Based upon the security services defined in TS 102 731 [1] and the security architecture define in TS 102 940 [5], it identifies the trust establishment and privacy management 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 [2].

The present document identifies and specifies security services for the establishment and maintenance of identities and cryptographic keys in an Intelligent Transport System (ITS). Its purpose is to provide the functions upon which systems of trust and privacy can be built within an ITS.

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 102 731: "Intelligent Transport Systems (ITS); Security; Security Services and Architecture".
 - [2] ETSI EN 302 665: "Intelligent Transport Systems (ITS); Communications Architecture".
 - [3] ETSI TS 102 867: "Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2".
 - [4] ETSI TS 102 942: "Intelligent Transport Systems (ITS); Security; Access control".
 - [5] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".
 - [6] ISO/IEC 8824-1:2008: "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation".
 - [7] ISO/IEC 8825-2:2008: "Information technology -- ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)".
 - [8] IEEE P1609.2/D12 (January 2012): "IEEE Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages".
- NOTE: Available from <http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?reload=true&punumber=6140528>.
- [9] ETSI TS 102 943: "Intelligent Transport Systems (ITS); Security; Confidentiality services".