

ETSI TS 102 731 V1.1.1 (2010-09)

Technical Specification

Intelligent Transport Systems (ITS); Security; Security Services and Architecture

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

[ETSI TS 102 731 V1.1.1 \(2010-09\)](https://standards.iteh.ai/catalog/standards/etsi/dcf6793a-a891-41a4-ac88-97ab037ab494/etsi-ts-102-731-v1-1-1-2010-09)

<https://standards.iteh.ai/catalog/standards/etsi/dcf6793a-a891-41a4-ac88-97ab037ab494/etsi-ts-102-731-v1-1-1-2010-09>



ReferenceDTS/ITS-0050001

Keywords

ITS, 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

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

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 2010.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™**, **TIPHON™**, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

LTE™ is a Trade Mark of ETSI currently being 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	6
Foreword.....	6
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	7
3 Definitions and abbreviations.....	8
3.1 Definitions.....	8
3.2 Abbreviations	9
4 Purpose of the Present Document	9
5 Refinement of Countermeasures	10
6 ITS Communications Security Architecture	14
6.1 Overview	14
6.2 ITS Authoritative Hierarchy.....	16
6.2.1 Overview	16
6.2.2 Manufacturer.....	16
6.2.3 Enrolment Authority	16
6.2.4 Authorization Authority.....	17
6.2.5 Trust Assumptions	18
6.2.5.1 Trust Assumptions in normal operation	18
6.2.5.2 Compromised ITS-S.....	19
6.2.5.3 Compromised Authorities	19
6.3 ITS Security Parameter Management.....	19
6.3.1 Identities and Identifiers in ITS	19
6.3.1.1 Authorization and privacy with authorization tickets	20
6.3.1.1.1 Personal user vehicles.....	20
6.3.1.1.2 Official role vehicles and infrastructure	20
6.3.1.2 Authorization tickets and cryptography for personal user vehicles and official role users	20
6.4 ITS Message Communication Models	21
6.4.1 Overview	21
6.4.2 Individual public messages	21
6.4.3 Individual private messages	21
6.4.4 Security Associations.....	21
7 ITS Security Services	22
7.1 Enrolment Credentials.....	22
7.1.1 Obtain Enrolment Credentials.....	22
7.1.1.1 Functional model.....	22
7.1.1.1.1 Functional model description	22
7.1.1.1.2 Description of functional entities	23
7.1.1.2 Information flows.....	23
7.1.1.2.1 Definition of information flows.....	23
7.1.2 Update Enrolment Credentials.....	26
7.1.2.1 Functional model.....	26
7.1.2.1.1 Functional model description	26
7.1.2.1.2 Description of functional entities	27
7.1.2.2 Information flows.....	27
7.1.2.2.1 Definition of information flows.....	27
7.1.2.2.2 Examples of information flow sequences.....	28
7.1.3 Remove Enrolment Credentials	29
7.1.3.1 Functional model.....	29
7.1.3.1.1 Functional model description	29
7.1.3.1.2 Description of functional entities	30

7.1.3.2	Information flows.....	30
7.1.3.2.1	Definition of information flows.....	30
7.1.3.2.2	Examples of information flow sequences.....	31
7.2	Authorization Tickets	32
7.2.1	Functional model	32
7.2.1.1	Functional model description	32
7.2.1.2	Description of functional entities	33
7.2.1.2.1	ITS Station Agent	33
7.2.1.2.2	A-Ticket Distributor	33
7.2.1.2.3	Enrolment Credentials Verifier	33
7.2.1.2.4	ITS Network Agent	33
7.2.1.2.5	ITS Authorization Status Manager	34
7.2.2	Obtain Authorization Tickets service	34
7.2.2.1	Information flows.....	34
7.2.2.1.1	Definition of information flows.....	34
7.2.3	Update Authorization Tickets	36
7.2.3.1	Functional model.....	36
7.2.3.1.1	Functional model description	36
7.2.3.2	Information flows.....	36
7.2.3.2.1	Definition of information flows.....	36
7.2.4	Publish Authorization Status.....	38
7.2.4.1	Information flows.....	38
7.2.4.1.1	Definition of information flows.....	38
7.2.5	Update Local Authorization Status Repository.....	40
7.2.5.1	Information flows.....	40
7.2.5.1.1	Definition of information flows.....	40
7.3	Security Associations	42
7.3.1	Model.....	42
7.3.1.1	Functional model.....	43
7.3.1.1.1	Functional model description	43
7.3.1.1.2	Description of functional entities	43
7.3.2	Establish Security Association.....	44
7.3.2.1	Information flows.....	44
7.3.2.1.1	Definition of information flows.....	44
7.3.3	Update security association.....	50
7.3.3.1	Information flows.....	50
7.3.3.1.1	Definition of information flows.....	50
7.3.4	Send Secured Message.....	54
7.3.5	Receive Secured Message.....	54
7.3.6	Remove security association.....	54
7.3.6.1	Information flows.....	54
7.3.6.1.1	Definition of information flows.....	54
7.4	Single message services	56
7.4.1	Authorize Single Message	56
7.4.2	Validate Authorization on Single Message.....	56
7.4.3	Encrypt Single Message.....	56
7.4.3.1	Overview.....	56
7.4.4	Decrypt Single Message	56
7.4.4.1	Overview.....	56
7.5	Integrity services	56
7.5.1	Calculate Check Value.....	56
7.5.2	Validate Check Value	56
7.5.3	Insert Check Value.....	57
7.6	Replay Protection services	57
7.6.1	Replay Protection Based on Timestamp	57
7.6.2	Replay Protection Based on Sequence Number.....	57
7.7	Accountability services	57
7.7.1	Record Incoming Message in Audit Log	57
7.7.2	Record outgoing message in Audit Log.....	57
7.8	Plausibility validation.....	57
7.8.1	Validate Data Plausibility	57
7.9	Remote management	58

7.9.1	Functional model	58
7.9.1.1	Functional model description	58
7.9.1.1.1	Description of functional entities	58
7.9.2	Activate ITS transmission.....	59
7.9.2.1	Information flows.....	59
7.9.2.1.1	Remote Activate Transmission.....	59
7.9.2.1.2	Activate Transmission	59
7.9.2.1.3	Transmission Activation.....	60
7.9.2.1.4	Examples of information flow sequences.....	60
7.9.3	Deactivate ITS transmission	61
7.9.3.1	Information flows.....	61
7.9.3.1.1	Definition of information flows.....	61
7.10	Report Misbehaving ITS-S.....	63
7.10.1	Report misbehaviour.....	63
7.10.1.1	Functional model.....	63
7.10.1.1.1	Functional model description	63
7.10.1.1.2	Description of functional entities	64
7.10.1.2	Information flows.....	64
7.10.1.2.1	Definition of information flows.....	64
Annex A (informative):	Bibliography.....	67
History		68

iTeh Standards

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

Document Preview

[ETSI TS 102 731 V1.1.1 \(2010-09\)](https://standards.iteh.ai/catalog/standards/etsi/dcf6793a-a891-41a4-ac88-97ab037ab494/etsi-ts-102-731-v1-1-1-2010-09)

<https://standards.iteh.ai/catalog/standards/etsi/dcf6793a-a891-41a4-ac88-97ab037ab494/etsi-ts-102-731-v1-1-1-2010-09>

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://webapp.etsi.org/IPR/home.asp>).

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 102 731 V1.1.1 \(2010-09\)](https://standards.iteh.ai/catalog/standards/etsi/dcf6793a-a891-41a4-ac88-97ab037ab494/etsi-ts-102-731-v1-1-1-2010-09)

<https://standards.iteh.ai/catalog/standards/etsi/dcf6793a-a891-41a4-ac88-97ab037ab494/etsi-ts-102-731-v1-1-1-2010-09>

1 Scope

The present document specifies mechanisms at the stage 2 level defined by ETS 300 387 [i.2] for secure and privacy-preserving communication in ITS environments. It describes facilities for credential and identity management, privacy and anonymity, integrity protection, authentication and authorization.

The mechanisms are specified as stage 2 security services according to the 3 stage method described in ETS 300 387 [i.2], and identify the functional entities and the information flow between them. The stage 2 security services will be refined into a number of security protocols as part of the stage 3 specifications. There may be several security protocols able to fulfil the requirements of a security services.

The present document describes the stage 2 security architecture of the ETSI Intelligent Transport System (ITS). The stage 2 security architecture and security services shall be used as the basis for further developing the ITS security architecture by mapping the security services and its functional components to the ITS architecture [i.7]. This mapping is part of stage 3 specifications.

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.

Not applicable.

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 102 893: "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)".
- [i.2] ETSI ETS 300 387: "Private Telecommunication Network (PTN); Method for the specification of basic and supplementary services".
- [i.3] United Nations General Assembly resolution 217 A (III) 10 December 1948: "Universal Declaration of Human Rights".
- [i.4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
- [i.5] COM 96/C 329/01: "European Union Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications".
- [i.6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.