ETSI TS 102 941 V2.2.1 (2022-11)

Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2

Reference
RTS/ITS-005102

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document specifies the trust and privacy management for Intelligent Transport Systems (ITS) communications. Based upon the security services defined in ETSI TS 102 731 [i.23] and the security architecture defined in ETSI 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 ETSI EN 302 665 [i.25].

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

2 References

2.1 Normative 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 https://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.

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

[1] Void.

[2] Void.

[3] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2".

[4] Void.

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

[6] ISO/IEC 8824-1:2021: "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation -- Part 1 Specification of basic notation".

[7] Recommendation ITU-T X.696 (02/2021): "Information technology - ASN.1 encoding rules: Specification of Octet Encoding Rules (OER)".

[8] Void.

[9] Void.

[10] Void.

[11] Void.

[12] Void.

[13] NIST FIPS PUB 198-1: "The Keyed-Hash Message Authentication Code (HMAC)".

[14] Void.

[15] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[16] ETSI TS 103 836-6-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols; Release 2".

[17] Void.

[18] ETSI TS 103 836-4-1: "Intelligent Transportation Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality; Release 2".

[19] ETSI TS 102 965: "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration; Release 2".

[20] Void.

[21] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

NOTE: Available from https://datatracker.ietf.org/doc/html/rfc5280.

[22] IETF RFC 5480: "Elliptic Curve Cryptography Subject Public Key Information".

NOTE: Available from https://www.rfc-editor.org/rfc/rfc5480.

[23] Void.

[24] IEEE 1609.2.1™-2022: "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities".

2.2 Informative 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.

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

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] ISO/IEC 15408-2: "Information technology -- Security techniques -- Evaluation criteria for IT security; Part 2: Security functional components".

[i.2] ETSI TR 102 638: "Intelligent Transport Systems (ITS); Vehicular communication; Basic Set of Applications; Release 2".

[i.3] IETF RFC 4046: "Multicast Security (MSEC) Group Key Management Architecture".

[i.4] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[i.5] IETF RFC 4302: "IP Authentication Header".

[i.6] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[i.7] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.8] IETF RFC 3547: "The Group Domain of Interpretation".

[i.9] IETF RFC 3830: "MIKEY: Multimedia Internet KEYing".

[i.10] IETF RFC 4535: "GSAKMP: Group Secure Association Key Management Protocol".

[i.11] IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol", December 2005.

[i.12] IETF RFC 4877: "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture".

[i.13] ETSI TS 102 723-8: "Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer".

[i.14] CVRIA: "Connected Vehicle Reference Implementation Architecture".

NOTE: Available at http://www.iteris.com/cvria/.

[i.15] ISO 21210-2010: "Intelligent Transport Systems (ITS) -- Communications access for land mobiles (CALM) -- Ipv6 networking".

[i.16] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[i.17] ETSI TS 102 942: "Intelligent Transport Systems (ITS); Security; Access control; Release 2".

[i.18] ETSI TS 102 943: "Intelligent Transport Systems (ITS); Security; Confidentiality services; Release 2".

[i.19] ETSI TS 103 900: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Specification of Cooperative Awareness Basic Service; Release 2".

[i.20] ETSI TS 103 831: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Decentralized Environmental Notification Service; Release 2".

[i.21] ETSI TS 103 301: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services; Release 2".

[i.22] IEEE 802.11™: "IEEE Standard for Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks-Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.23] ETSI TS 102 731: "Intelligent Transport Systems (ITS); Security; Security Services and Architecture; Release 2".

[i.24] Void.

[i.25] ETSI EN 302 665: "Intelligent Transport Systems (ITS); Communications Architecture".

[i.26] EU C-ITS Security Credential Management System (EU CCMS).

3 Definition of terms, symbols, abbreviations and notation

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 102 731 [i.23], ETSI TS 102 940 [5], ISO/IEC 15408-2 [i.1] and the following apply:

delta CTL: partial CTL that only contains CTL entries that have been updated since the issuance of the prior, base CTL

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 103 097 [3], ETSI TS 102 940 [5], ETSI TS 103 836-4-1 [18] and the following apply:

AA	Authorization Authority
AES	Advanced Encryption Standard
ASN	Abstract Syntax Notation
AT	Authorization Ticket
CA	Certification Authority
CCH	Control CHannel
CCM	Counter with CBC-MAC
CCMS	Cooperative-ITS Certificate Management System
COER	Canonical Octet Encoding Rules
CPOC	C-ITS Point Of Contact
CRL	Certificate Revocation List
CTL	Certificate Trust List
CVRIA	Connected Vehicle Reference Implementation Architecture
DC	Distribution Centre
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
EC	Enrolment Credential
ECC	Elliptic Curve Cryptography
ECTL	European Certificate Trust List
EV	Electric Vehicle
FIPS	Federal Information Processing Standard
GET	command HTTP GET
GN/BTP	GeoNetworking/Basic Transport Protocol
GN6	GeoNetworking-IPv6
HMAC	keyed-Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITS-AID	ITS Application ID
ITU-T	International Telecommunication Union - Telecommunication standardization sector
KDF	Key Derivation Function
LTE	Long Term Evolution (4G)
MSB	Most Significant Bit
MSEC	Multicast SECurity
OBD	On-Board Diagnosis
PA	Policy Authority
PDU	Protocol Data Unit
PII	Personally Identifiable Information
POP	Proof Of Possession
PSID	Provider Service Identifier
RCA	Root Certification Authority
RFC	Request For Comment
SA	Security Association
SCH	Service CHannel
SLAAC	StateLess Address Auto Configuration
SM	Security Management
SSP	Service Specific Permissions
TCP	Transmission Control Protocol
TLM	Trust List Manager
TLS	Transport Layer Security
URL	Uniform Resource Locator
V2I	Vehicle-to-Infrastructure
WLAN	Wireless Local Area Network
XOR	eXclusive OR function

3.4 Notation

The requirements identified in the present document include:

a) mandatory requirements strictly to be followed in order to conform to the present document. Such requirements are indicated by clauses without any additional marking;

b) requirements strictly to be followed if applicable to the type of ITS Station concerned.

Such requirements are indicated by clauses marked by "[CONDITIONAL]"; and where relevant is marked by an identifier of the type of ITS-S for which the clauses are applicable as follows:

- [Itss_WithPrivacy] is used to denote requirements applicable to ITS-S for which pseudonymity has to be assured and re-identification by the AA is not allowed. This includes for instance personal user vehicle ITS-S or personal ITS-S Portable.
- [Itss_NoPrivacy] is used to denote requirements applicable to ITS-S for which pseudonymity does not have to be assured and are allowed to be re-identified by the AA. This may be for instance fixed or mobile RSUs or special vehicles.

4 ITS authority hierarchy

Trust and privacy management requires secure distribution and maintenance (including revocation when applicable) of trust relationships, which may be enabled by specific security parameters that include enrolment credentials that provide 3rd party certificates of proof of identity or other attributes such as pseudonym certificates. Public key certificates and Public Key Infrastructure (PKI) are used to establish and maintain trust between the ITS-S and other ITS-S and authorities.

ETSI TS 102 731 [i.23] specifies requirements on security management services and security management roles such as EAs and AAs. The ITS security architecture is defined in ETSI TS 102 940 [5] and covers both the secured Communication Architecture, the architecture of the ITS-S Communication security system and the Security Management System architecture.

The present document assumes the definition of the security management entities specified in ETSI TS 102 940 [5] and the top-level entities for the management of multiple Root CAs collaborating within a single Trust Model.

5 Privacy in ITS

ISO/IEC 15408-2 [i.1] identifies 4 key attributes that relate to privacy:

- anonymity;
- pseudonymity;
- unlinkability; and
- unobservability.

Anonymity alone is insufficient for protection of an ITS user's privacy and unsuitable as a solution for ITS, as one of the main requirements of ITS is that the ITS-S should be observable in order to provide improved safety. Consequently, pseudonymity and unlinkability offer the appropriate protection of the privacy of a sender of basic ITS safety messages (CAM and DENM). Pseudonymity ensures that an ITS-S may use a resource or service without disclosing its identity but can still be accountable for that use [i.1]. Unlinkability ensures that an ITS-S may make multiple uses of resources or services without others being able to link them together [i.1].

Pseudonymity shall be provided by using temporary identifiers in ITS safety messages, and never transmitting the station's canonical identifier in communications between ITS stations. Unlinkability can be achieved by limiting the amount of detailed immutable (or slowly changing) information carried in the ITS safety message, thus preventing the possible association of transmissions from the same vehicle over a long time period (such as two similar transmissions broadcast on different days).

ITS Privacy is provided in two dimensions:

i) privacy of ITS registration and authorization tickets provisioning:

   - ensured by permitting knowledge of the canonical identifier of an ITS-S to only a limited number of authorities (EAs);

   - provided by the separation of the duties and roles of PKI authorities into an entity verifying the canonical identifier known as the Enrolment Authority (EA) and an entity responsible for authorizing and managing services known as the Authorization Authority (AA);

ii) privacy of communications between ITS-Ss.

Separation of duties for enrolment (identification and authentication) and for authorization has been shown in ETSI TS 102 731 [i.23] as an essential component of privacy management and provides protection against attacks on a user's privacy. However, it is possible for the EA role to be delegated to the manufacturer and for the EA and AA roles to be assumed by a single authority.

When the same operational authority manages both the EA and AA, it shall guarantee privacy of requesting ITS-S i.e. providing all the technical and organizational measures to ensure that ITS identity information held by the EA is kept separately to avoid re-identification of pseudonym certificates (ATs).

When dedicated authorities are used only for certificates provisioning to ITS-S which do not have privacy requirements such as Road-Side Units, the EA and AA may not provide technical and operational separation.

6 Trust and privacy management

6.1 ITS-S Security Lifecycle

6.1.1 ITS-S Life-cycle management

The ITS-S Security Lifecycle includes the following stages (see Figure 1):

- initial ITS-S configuration during manufacture;
- enrolment;
- authorization;
- operation and maintenance;
- end of life.

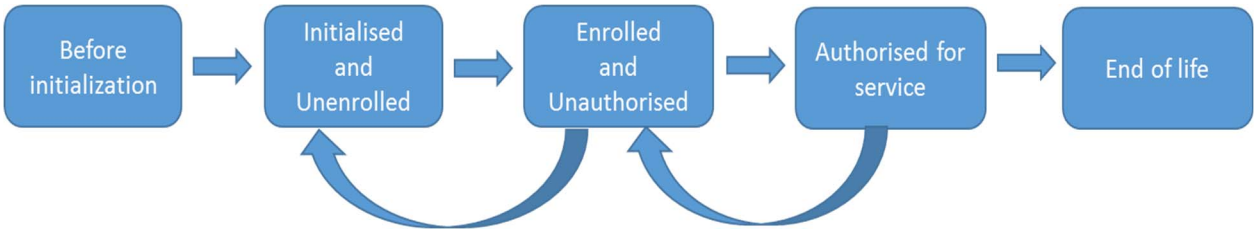

Figure 1: ITS Station Security Life Cycle

6.1.2 Manufacture

As part of the ITS-S manufacturing process, the following information elements associated with the identity of the station shall be established within the ITS-S itself and within the Enrolment Authority (EA):

- In the ITS-S, the following information elements shall be established using a physically secure process. The specification of this physically secure process is out of scope for the present document:
  - a canonical identifier which is globally unique (see note 1);
  - contact information for the EA and AA which will issue certificates for the ITS-S:
    - network address;
    - public key certificate;
  - the set of current known trusted AA certificates which the ITS-S may use to trust communications from other ITS-S;
  - when using the process specified in clause 6.2.3.2 for the initial enrolment: a public/private key pair for cryptographic purposes (canonical key pair); and
  - the trust anchor (Root CA) public key certificate and the DC network address;
  - in case of a multiple root CAs architecture as specified in ETSI TS 102 940 [5], the TLM public key certificate and the CPOC network address.

NOTE 1: The management of the canonical identifier and the means to guarantee uniqueness are not addressed in the present document.

- In the EA, the following three items of information shall be established, all associated with each other (see note 2):
  - the permanent canonical identifier of the ITS-S;
  - the profile information for the ITS-S that may contain an initial list of maximum appPermissions (ITS-AIDs with SSP), region restrictions and assurance level which may be modified over time;
  - when using the process specified in clause 6.2.3.2 for the initial enrolment: the public key from the key pair belonging to the ITS-S (canonical public key).

NOTE 2: The process for establishing this information within the ITS-S and the EA is beyond the scope of the present document.

NOTE 3: The EA certificate may contain `certIssuePermissions` with type `enrol` limiting the maximum permissions (ITS-AIDs with SSP) assigned to the ITS-S in the profile information. In this case, the Root CA (issuer of the EA certificate) contains at least these `certIssuePermissions` with type `enrol` in its certIssuePermissions.

6.1.3 Enrolment

6.1.3.0 General Considerations

There are two types of enrolment certificate that can be used to authenticate requests for authorization tickets:

- ETSI TS 102 941 enrolment credentials following the specification in the present document. The provisioning of this type is described in the present document.
- X.509 enrolment credentials following the X.509 format which is specified in IETF RFC 5280 [21] and IETF RFC 5480 [22]. The provisioning of this type is out-of-scope of the present document since mechanisms already exist. The present document will explicitly refer to X.509 enrolment credentials when this type is meant.

The following process applies to the provisioning of ETSI TS 102 941 enrolment credentials.

The ITS-S requests its enrolment certificate from the EA (see clause 6.2.3.2).

When an end entity applies for an enrolment certificate, it may indicate that it is entitled to the certificate *directly* or *indirectly*. Compare with section 4.1.4.2 of IEEE 1609.2.1 [24].

In the *indirect* initial enrolment case, the Enrolment Authority (EA) is given assurance that the end entity is entitled to the enrolment certificate by means outside the scope of the enrolment certificate request. For example, the enrolment request could happen in an environment that is trusted by the EA and the request could be transmitted over a secure connection.

In the *direct* initial enrolment case, before enrolment happens, the end entity generates a keypair known as the canonical keypair and is assigned (or generates) a globally unique identifier known as the canonical identity (see clause 6.1.2).

The state transitions for enrolment are shown in Figure 2.

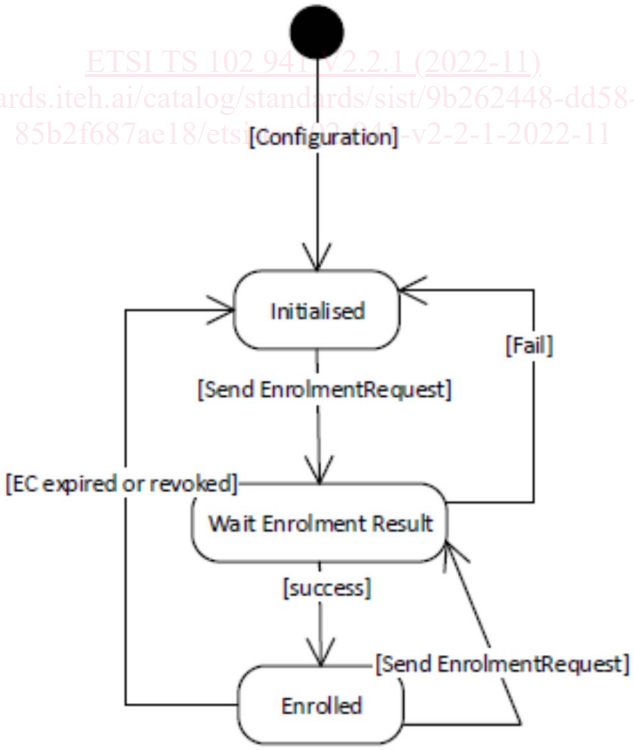

Figure 2: Simplified state machine for the enrolment process

After a successful enrolment process, the ITS-S shall possess an enrolment credential that shall be used in subsequent authorization requests.

For renewing the Enrolment Certificate at the EA, the ITS-S shall send an EnrolmentRequest signed by the previous valid enrolment credential issued by this EA.

6.1.3.1 Enrolment Credential Profile

6.1.3.1.0 Introduction

The profile for the ETSI enrolment credential is defined in ETSI TS 103 097 [3] along with the ETSI ITS security header and certificate format.

Since the format of the X.509 enrolment credential is not defined in ETSI TS 103 097 [3] but used for trust and privacy management in the present document, the profile for X.509 enrolment credentials is specified in the present document.

The X.509 enrolment credential shall apply the following conditions. Additional conditions may be required by the individual X.509 PKI in alignment with the Enrolment Authority.

6.1.3.1.1 Generic Requirements

The certificate shall follow the IETF PKIX profile as specified in IETF RFC 5280 [21]. When ECDSA keys are used, the encoding shall follow the specification in IETF RFC 5480 [22]. The cryptographic algorithms shall be aligned with ETSI TS 103 097 [3].

6.1.3.1.2 Version

The version shall be V3 (defined by the integer value 2).

6.1.3.1.3 Issuer

The identity of the issuer shall contain at least the following attributes:

- countryName;
- organizationName; and
- commonName.

Each attribute shall be limited to a single instance of the attribute. Additional attributes may be present.

The countryName attribute shall specify the country in which the issuer of the certificate is established.

The organizationName attribute shall contain the full registered name of the certificate issuing organization.

The commonName attribute value shall contain a name commonly used by the subject to represent itself. This name need not be an exact match of the fully registered organization name.

6.1.3.1.4 Subject

The subject field shall include at least the following attributes:

- countryName;
- organizationName; and
- commonName.

Only one instance of each of these attributes shall be present. Additional attributes may be present.

The countryName attribute shall specify the country in which the ITS-S is established.

The organizationName attribute shall contain the full registered name of the ITS-S.

The commonName attribute value shall contain a name commonly used by the subject to represent itself and may correspond to the canonical ID.