ETSI TS 103 097 V1.3.1 (2017-10)

Intelligent Transport Systems (ITS);
Security;
Security header and certificate formats

Reference
RTS/ITS-00540

Keywords
ITS, privacy, protocol, 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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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 https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

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 (https://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.

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.

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.

Introduction

Security policies require that data structures such as messages used in Intelligent Transport Systems are secured when stored or transferred. For interoperability reasons, a common format for secure data structures featuring security headers and public key certificates needs to be provided.

The present document provides these definitions as a profile of the base standard IEEE Std 1609.2™-2016 and its amendment IEEE 1609.2a™-2017 [1]. A profile makes use of the definitions in the base standard and defines the use of particular subsets or options available in the base standard. This implies that the present document is to be read and interpreted together with that base standard.

The present document contains material from IEEE Std 1609.2-2016 [1] and its amendment(s), reprinted with permission from IEEE, and Copyright © 2016.

1 Scope

The present document specifies the secure data structure including header and certificate formats for Intelligent Transport Systems.

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] IEEE Std 1609.2™-2016: "IEEE Standard for Wireless Access in Vehicular Environments -- Security Services for Applications and Management Messages", as amended by IEEE Std 1609.2a™-2017: "Standard for Wireless Access In Vehicular Environments -- Security Services for Applications and Management Messages Amendment 1".

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

[3] Recommendation ITU-T X.696 (08/2014): "Information Technology-Specification of Octet Encoding Rules (OER)".

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

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

3 Abbreviations

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

AA	Authorization Authority
ASN.1	Abstract Syntax Notation One
AT	Authorization Ticket

CA	Certification Authority
CAM	Cooperative Awareness Message
COER	Canonical Octet Encoding Rules
CRL	Certificate Revocation List
CTL	Certificate Trust List
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
ITS	Intelligent Transport Systems
ITS-AID	ITS Application ID
ITS-S	Intelligent Transport Systems Station
SSP	Service Specific Permissions
TLM	Trust List Manager

4 Basic format elements

Data structures in the present document are defined using Abstract Syntax Notation 1 (ASN.1) and shall be encoded using the Canonical Octet Encoding Rules (COER) as defined in Recommendation ITU-T X.696 [3]. This includes some data structures in the present document for which a "canonical encoding" is used as defined in IEEE Std 1609.2 [1].

Clause 5 and 6 specify and describe the data structures with reference to IEEE Std 1609.2 [1]. The corresponding ASN.1 module is defined in annex A.

The validity of a certificate shall be assessed as defined in IEEE Std 1609.2 [1] clause 5.1, using the Hash ID-based revocation method for EA and AA certificates, and no revocation method for authorization tickets and enrolment credentials.

NOTE 1: The CRL for EA and AA certificates is defined in ETSI TS 102 941 [i.2].

NOTE 2: The rules for verification of the Root CA certificate against the CTL are defined in ETSI TS 102 941 [i.2].

The validity of signed data shall be assessed as defined in IEEE Std 1609.2 [1] clause 5.2.

5 Specification of secure data structure

5.1 EtsiTs103097Data

A secure data structure shall be of type `EtsiTs103097Data` as defined in annex A, which corresponds to a `Ieee1609Dot2Data` as defined in IEEE Std 1609.2 [1] clause 6.3.2, with the constraints defined in this clause, in clause 5.2 and in clause 5.3.

The type `Ieee1609Dot2Data` shall support the following options in the component content:

- The option `unsecuredData` shall be used to encapsulate an unsecured data structure.
- The option `signedData`, corresponding to the type `SignedData` as defined in IEEE Std 1609.2 [1] clause 6.3.4, shall be used to transfer a data structure with a signature.
- The option `encryptedData`, corresponding to the type `EncryptedData` as defined in IEEE Std 1609.2 [1] clause 6.3.30, shall be used to transfer an encrypted data structure.

The following corresponding profiles of the type `EtsiTs103097Data` are defined in annex A:

- The parameterized type `EtsiTs103097Data-Signed` using the Ieee1609Dot2Data option `signedData` containing the data structure in the component tbdData.payload.data.

- The parameterized type EtsiTs103097Data-SignedExternalPayload using the Ieee1609Dot2Data option signedData containing the digest of the data structure in the component tbdData.payload.extDataHash.

- The parameterized type EtsiTs103097Data-Encrypted, using the Ieee1609Dot2Data option encryptedData containing the encrypted data structure in the component ciphertext.aes128ccm.ccmCiphertext.

- The parameterized type EtsiTs103097Data- SignedAndEncrypted, using the Ieee1609Dot2Data option EncryptedData, containing an encrypted EtsiTs103097Data-Signed.

5.2 SignedData

The type SignedData shall have the following constraints:

The component hashId of SignedData shall indicate the hash algorithm to be used to generate the hash of the message according to IEEE Std 1609.2 [1] clauses 6.3.5 and 5.3.3.

The component tbsData of SignedData shall be of type ToBeSignedData as defined in IEEE Std 1609.2 [1] clause 6.3.6. The type ToBeSignedData shall have the component payload of type SignedDataPayload as defined in IEEE Std 1609.2 [1] clause 6.3.7, containing either:

- the component data, containing the payload to be signed as an Ieee1609Dot2Data, or

- the component extDataHash, containing the hash of data that is not explicitly transported within the structure.

The type ToBeSignedData shall have the component headerInfo of type HeaderInfo as defined in IEEE Std 1609.2 [1] clause 6.3.9, and constrained to have the following security headers:

- The component psid containing the ITS-AID corresponding to the contained message.

- The component generationTime as defined in IEEE Std 1609.2 [1], always present.

- The component expiryTime, as defined in IEEE Std 1609.2 [1], present or absent according to the specification of message profiles in clause 7.

- The component generationLocation, as defined in IEEE Std 1609.2 [1], present or absent according to the specification of message profiles in clause 7.

- The component p2pcdLearningRequest always absent.

- The component missingCrlIdentifier always absent.

- The component encryptionKey, as defined in IEEE Std 1609.2 [1], present or absent according to the specification of message profiles in clause 7.

- The component inlineP2pcdRequest, as defined in IEEE Std 1609.2 [1], present or absent according to the specification of message profiles in clause 7.

- The component requestedCertificate, as defined in IEEE Std 1609.2 [1], present or absent according to the specification of message profiles in clause 7.

The component signer of SignedData shall be of type SignerIdentifier as defined in IEEE Std 1609.2 [1] clause 6.3.24, and constrained to one of the following choices:

- digest, containing the digest of the signing certificate as defined in IEEE Std 1609.2 [1] clause 6.3.26.

- certificate, constrained to only one entry in the SequenceOfCertificate list of type TS103097Certificate, containing the signing certificate as defined in clause 6 of the present document.

The component `signature` of `SignedData` shall be of type `Signature` as defined in IEEE Std 1609.2 [1] clause 6.3.28 and shall contain the ECDSA signature as defined in IEEE Std 1609.2 [1] clauses 6.3.29, 6.3.29a and 5.3.1.

5.3 EncryptedData

The type `EncryptedData` shall have the following constraints:

The component `recipients` of `EncryptedData` shall be of type `SequenceOfRecipientInfo` as defined in IEEE Std 1609.2 [1] clause 6.3.31. Every entry shall be either of option `pskRecipInfo` as defined in IEEE Std 1609.2 [1] clause 6.3.32, of option `certRecipInfo`, or of option `signedDataRecipInfo`, as defined in IEEE Std 1609.2 [1] clause 6.3.34.

The encryption scheme used shall be ECIES as defined in IEEE Std 1609.2 [1] clause 5.3.5. The component `ciphertext` of `EncryptedData` shall be of type `SymmetricCiphertext` as defined in IEEE Std 1609.2 [1] clause 6.3.37 and contain a `EtsiTs103097Data` encrypted according to IEEE Std 1609.2 [1] clauses 6.3.38 and 5.3.8.

6 Specification of certificate format

A certificate contained in a secure data structure shall be of type `EtsiTs103097Certificate` as defined in annex A, which corresponds to a single `ExplicitCertificate` as defined in IEEE Std 1609.2 [1] clause 6.4.6, with the constraints defined in this clause.

The component `toBeSigned` of the type `EtsiTs103097Certificate` shall be of type `ToBeSignedCertificate` as defined in IEEE Std 1609.2 [1] clause 6.4.8 and constrained as follows:

- The component `id` of type `CertificateId` constrained to choice type `name` or `none`.
- The component `cracaId` set to 000000'H.
- The component `crlSeries` set to 0'D.
- The component `validityPeriod` with no further constraints.
- The component `region` of type `GeographicRegion` as defined in IEEE Std 1609.2 [1], present or absent according to the specification of certificate profiles in clause 7.
- The component `assuranceLevel` of type `SubjectAssurance`, as defined in IEEE Std 1609.2 [1], present or absent according to the specification of certificate profiles in clause 7.
- The component `appPermissions` of type `SequenceOfPsidSsp` as defined in IEEE Std 1609.2 [1], present or absent according to the specification of certificate profiles in clause 7.
- The component `certIssuePermissions` of type `SequenceOfPsidGroupPermissions`, as defined in IEEE Std 1609.2 [1], present or absent according to the specification of certificate profiles in clause 7.
- At least one of the components `appPermissions` and `certIssuePermissions` shall be present.
- The component `certRequestPermissions` absent.
- The component `canRequestRollover` absent.
- The component `encryptionKey` of type `PublicEncryptionKey` as defined in IEEE Std 1609.2 [1], present or absent according to the specification of certificate profiles in clause 7.
- The component `verifyKeyIndicator` of type `VerificationKeyIndicator` as defined in IEEE Std 1609.2 [1], present and constrained to the choice verificationKey.

The component signature of EtsiTs103097Certificate shall be of type Signature as defined in IEEE Std 1609.2 [1] clause 6.3.28 and shall contain the signature, calculated by the signer identified in the issuer component, as defined in IEEE Std 1609.2 [1] clauses 6.3.29, 6.3.29a and 5.3.1.

7 Security profiles

7.1 Profiles for messages

7.1.1 Security profile for CAMs

The secure data structure containing Cooperative Awareness Messages (CAMs) shall be of type EtsiTs103097Data-Signed as defined in clause 5.1 and annex A, containing the CAM as the ToBeSignedDataContent, with the additional constraints defined in clause 5.2 and this clause:

- The component signer of SignedData shall be constrained as follows:
  - As default, the choice digest shall be included.
  - The choice certificate shall be included once, one second after the last inclusion of the choice certificate.
  - If the ITS-S receives a CAM signed by a previously unknown AT, it shall include the choice certificate immediately in its next CAM, instead of including the choice digest. In this case, the timer for the next inclusion of the choice certificate shall be restarted.
  - If an ITS-S receives a CAM that includes a tbsdata.headerInfo component of type inlineP2pcdRequest, then the ITS-S shall evaluate the list of certificate digests included in that component: If the ITS-S finds a certificate digest of the currently used authorization ticket in that list, it shall include a the choice certificate immediately in its next CAM, instead of including the choice digest.
- The component tbsdata.headerInfo of SignedData shall be further constrained as follows:
  - psid: this component shall encode the ITS-AID value for CAMs as assigned in ETSI TS 102 965 [2].
  - The component inlineP2pcdRequest shall be included and shall contain the digests of certificates currently unknown to the ITS-Station in the following cases:
    - if the ITS-S received a CAM with the component signer of SignedData set to the choice digest, and this digest points to an unknown authorization ticket;
    - if the ITS-S received a message with the component signer of SignedData set to the choice certificate, and this certificate is signed by an unknown authorization authority certificate, i.e. includes the component issuer referencing an unknown certificate.
  - requestedCertificate: If an ITS-S receives a CAM with the component tbsdata.headerInfo including a the component inlineP2pcdRequest, then the ITS-S shall evaluate the list of digests included in that component: If the ITS-S finds a digest of a valid certification authority certificate, it shall include the component requestedCertificate containing the requested certificate immediately in its next CAM:
    - unless before the generation of the next CAM, the ITS-S received another CAM including the component requestedCertificate containing the requested certification authority certificate: in this case the request shall be discarded;
    - unless the component signer of SignedData is of choice certificate according to the rules defined above: in this case the request shall be kept pending and the certificate shall be inserted in the next possible CAM, according to the same conditions.

- All other components of the component `tbsdata.headerInfo` allowed to be present according to clause 5 shall not be used and be absent.

7.1.2 Security profile for DENMs

The secure data structure containing Decentralized Environmental Notification Messages (DENMs) shall be of type `EtsiTs103097Data-Signed` as defined in clause 5.1 and annex A, containing the DENM as the `ToBeSignedDataContent`, with the additional constraints defined clause 5.2 and in this clause:

- The component `signer` of `SignedData` shall be of choice `certificate`.
- The component `tbsdata.headerInfo` of SignedData shall be further constrained as follows:
  - `generationLocation`: shall be present.
  - `psid`: this component shall encode the ITS-AID value for DENMs as assigned in ETSI TS 102 965 [2].
- All other components of the component `tbsdata.headerInfo` allowed to present according to clause 5 shall not be used and be absent.

7.1.3 Generic security profile for other signed messages

The secure data structure containing signed messages other than CAM and DENM shall be of type:

- `EtsiTs103097Data-Signed` as defined in clause 5.1 and annex A, containing the message as the `ToBeSignedDataContent`, or of type;
- `EtsiTs103097Data-SignedExternalPayload` as defined clause 5.1 and in annex A, containing the message digest;

with the additional constraints defined in clause 5.2.

7.1.4 Security profile for encrypted messages

The secure data structure containing encrypted messages shall be of type `EtsiTs103097Data-Encrypted` as defined in clause 5.1 and annex A, containing the message as the `ToBeEncryptedDataContent`, with the additional constraints defined in clause 5.3.

7.1.5 Security profile for signed and encrypted messages

The secure data structure containing signed and then encrypted messages shall be of type `EtsiTs103097Data-SignedAndEncrypted` as defined in clause 5.1 and annex A, containing the message as the `ToBesignedAndEncryptedDataContent`. This corresponds to a `EtsiTs103097Data` of type `EtsiTs103097Data-Encrypted`, containing a EtsiTs103097Data of type `EtsiTs103097Data-Signed`, containing the message as the `ToBeSignedDataContent`.

7.2 Profiles for certificates

7.2.1 Authorization tickets

This clause defines additional aspects of authorization tickets as defined in ETSI TS 102 940 [i.1]. Authorization tickets shall be of type `EtsiTs103097Certificate` as defined in clause 6, with the following constraints:

The component `issuer` shall be of choice `sha256AndDigest` or `sha384AndDigest` as defined in IEEE Std 1609.2 [1] clause 6.4.7.

The `toBeSigned` component `appPermissions` shall be used to indicate message signing permissions, i.e. permissions to sign a `EtsiTs103097Data`.